Kerstin Zettl-Schabath

Staatliche Cyberkonflikte

Proxy-Strategien von Autokratien und Demokratien im Vergleich



[transcript] Politik in der digitalen Gesellschaft

Kerstin Zettl-Schabath
Staatliche Cyberkonflikte

Politik in der digitalen Gesellschaft | Band 6

Die freie Verfügbarkeit der E-Book-Ausgabe dieser Publikation wurde ermöglicht durch **POLLUX – Informationsdienst Politikwissenschaft**



und die Open Library Community Politik 2023 – einem Netzwerk wissenschaftlicher Bibliotheken zur Förderung von Open Access in den Sozial- und Geisteswissenschaften:

Hauptsponsor: Fachinformationsdienst Politikwissenschaft – POLLUX

Vollsponsoren: Technische Universität Braunschweig | Carl von Ossietzky-Universität Oldenburg | Universiätsbibliothek der FernUniversität Hagen | Freie Universität Berlin – Universitätsbibliothek | Niedersächsische Staats- und Universitätsbibliothek Göttingen | Goethe-Universität Frankfurt am Main | Gottfried Wilhelm Leibniz Bibliothek – Niedersächsische Landesbibliothek | TIB – Leibniz-Informationszentrum Technik und Naturwissenschaften und Universitätsbibliothek | Humboldt-Universität zu Berlin | Justus-Liebig-Universität Gießen | Universitätsbibliothek Eichstätt-Ingolstadt | Ludwig-Maximilians-Universität München | Max Planck Digital Library (MPDL) | Rheinische Friedrich-Wilhelms-Universität Bonn | Ruhr-Universität Bochum | Staats- und Universitätsbibliothek Carl von Ossietzky, Hamburg | SLUB Dresden | Staatsbibliothek zu Berlin | Universitätsbibliothek Chemnitz | Universitäts- und Landesbibliothek Darmstadt | Universitätsbibliothek „Georgius Agricola“ der TU Bergakademie Freiberg | Universitätsbibliothek Kiel (CAU) | Universitätsbibliothek Leipzig | Universität Wien | Universitäts- und Landesbibliothek Düsseldorf | Universitäts- und Landesbibliothek Münster | Universitäts- und Stadtbibliothek Köln | Universitätsbibliothek Bielefeld | Universitätsbibliothek der Bauhaus-Universität Weimar | Universitätsbibliothek Kassel | Universitätsbibliothek Osnabrück | Universitätsbibliothek St. Gallen | Universitätsbibliothek Vechta | Vorarlberger Landesbibliothek | Zentral- und Hochschulbibliothek Luzern | Zentralbibliothek Zürich | ZHAW Zürcher Hochschule für Angewandte Wissenschaften, Hochschulbibliothek

Sponsoring Light: Bundesministerium der Verteidigung | Bibliothek der Hochschule für Technik und Wirtschaft Dresden | Bibliothek der Hochschule für Technik, Wirtschaft und Kultur Leipzig | Bibliothek der Westsächsischen Hochschule Zwickau | Bibliothek der Hochschule Zittau/Görlitz | Hochschulbibliothek der Hochschule Mittweida | Institut für Auslandsbeziehungen (IfA) | Landesbibliothek Oldenburg | Österreichische Parlamentsbibliothek

Mikrosponsoring: Bibliothek der Berufsakademie Sachsen | Bibliothek der Evangelische Hochschule Dresden | Bibliothek der Hochschule für Musik und Theater „Felix Mendelssohn Bartholdy“ Leipzig | Bibliothek der Hochschule für Bildende Künste Dresden | Bibliothek der Hochschule für Musik „Carl Maria von Weber“ Dresden | Bibliothek der Hochschule für Grafik und Buchkunst Leipzig | Bibliothek der Palucca-Hochschule für Tanz Dresden | Leibniz-Institut für Europäische Geschichte | Stiftung Wissenschaft und Politik (SWP) – Deutsches Institut für Internationale Politik und Sicherheit

Kerstin Zettl-Schabath

Staatliche Cyberkonflikte

Proxy-Strategien von Autokratien und Demokratien im Vergleich

[transcript]

Diese Studie wurde 2022 unter dem Titel »Proxys im staatlichen Cyberkonfliktaustrag: Eine vergleichende Analyse der VR China, Russlands, der USA und Israels« an der Fakultät für Wirtschafts- und Sozialwissenschaften der Ruprecht-Karls-Universität Heidelberg als Dissertation angenommen.
Gutachter: Prof. Dr. Sebastian Harnisch, Prof. Dr. Wolf J. Schünemann

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.



Dieses Werk ist lizenziert unter der Creative Commons Attribution-ShareAlike 4.0 Lizenz (BY-SA). Diese Lizenz erlaubt unter Voraussetzung der Namensnennung des Urhebers die Bearbeitung, Vervielfältigung und Verbreitung des Materials in jedem Format oder Medium für beliebige Zwecke, auch kommerziell, sofern der neu entstandene Text unter derselben Lizenz wie das Original verbreitet wird.
Die Bedingungen der Creative-Commons-Lizenz gelten nur für Originalmaterial. Die Wiederverwendung von Material aus anderen Quellen (gekennzeichnet mit Quellenangabe) wie z.B. Schaubilder, Abbildungen, Fotos und Textauszüge erfordert ggf. weitere Nutzungsgenehmigungen durch den jeweiligen Rechteinhaber.

Erschienen 2023 im transcript Verlag, Bielefeld
© Kerstin Zettl-Schabath

Umschlaggestaltung: Maria Arndt, Bielefeld
Druck: Majuskel Medienproduktion GmbH, Wetzlar
https://doi.org/10.14361/9783839468883
Print-ISBN: 978-3-8376-6888-9
PDF-ISBN: 978-3-8394-6888-3
EPUB-ISBN: 978-3-7328-6888-9
Buchreihen-ISSN: 2699-6626
Buchreihen-eISSN: 2703-111X

Gedruckt auf alterungsbeständigem Papier mit chlorfrei gebleichtem Zellstoff.
Besuchen Sie uns im Internet: *https://www.transcript-verlag.de*
Unsere aktuelle Vorschau finden Sie unter *www.transcript-verlag.de/vorschau-download*

Inhalt

Vorwort

Diese Studie habe ich im Rahmen meiner Promotion am Institut für Politische Wissenschaft der Universität Heidelberg erarbeitet. Sie behandelt den Zeitraum von 2000 bis Ende 2021, weshalb die Entwicklungen rund um den Ukraine-Krieg seit Februar 2022 kein Kernbestandteil der Arbeit sind. Die seither zunehmende Involvierung russischer Cyber-Crime-Gruppierungen in »patriotisches Hacking«, sowie auf Seiten der Ukraine staatlich initiierter »Cyber-Freiwilligenverbände« wie der IT Army of Ukraine, unterstreichen jedoch die (immer noch oder wieder) bedeutende Rolle nichtstaatlicher Akteure im Rahmen staatlichen Cyberkonfliktaustrags. Ferner könnten private Unternehmen wie Microsoft, Google oder auch Starlink, die die Ukraine seit Kriegsbeginn (und in Teilen auch schon zuvor) bei ihren (Cyber-)abwehr-Bemühungen unterstützt haben, ebenfalls als »defensive Cyberproxys« demokratischer Staaten bezeichnet werden. Neben der Attribution von Cyberangriffen durch private IT-Unternehmen kann das in dieser Arbeit entwickelte Erklärungsmodell somit auch auf weitere Kontexte Anwendung finden.

An dieser Stelle möchte ich mich bei all den Personen bedanken, die mich auf diesem Weg in den letzten Jahren begleitet und unterstützt haben.

Mein erster und größter Dank gilt meinem Betreuer, Prof. Dr. Sebastian Harnisch, der mich von Beginn an motiviert und unterstützt hat. Dieser stetige und intensive inhaltliche Austausch ist in dieser Form sicherlich nicht selbstverständlich. Eine solch umfassende, konstruktive, stets menschliche sowie auch persönlich weiterbringende Betreuung kann ich nur jedem Doktoranden und jeder Doktorandin wünschen. Vielen Dank dafür!

Ebenso möchte ich mich bei Prof. Dr. Wolf J. Schünemann dafür bedanken, dass er sich sofort bereit erklärt hat, als mein Zweitgutachter zu fungieren. Auch das in seinem PhD-Kolloquium von ihm selbst sowie seinen DoktorandInnen erhaltene Feedback habe ich als sehr wertvoll bei der Erstellung dieser Arbeit empfunden.

Mein großer Dank gilt zudem Dr. Stefan Steiger, der mich auch dann noch mit Rat und Tat bei der Entwicklung und Fertigstellung des Heidelberger Konfliktdatensatzes, sowie dieser Arbeit unterstützt hat, als er schon längst in Hildesheim tätig war. Dabei konnte ich viel von seinem technischen Wissen profitieren.

Auch die zahlreichen Gespräche mit meinen KollegInnen des Lehrstuhls von Prof. Harnisch, besonders Fanny Schardey und Tijana Lujic, waren sehr wichtig in den ver-

schiedenen Phasen meiner Promotion, inhaltlich und persönlich. Ich bin beiden zudem sehr dankbar für ihre zahlreichen kritischen, jedoch stets konstruktiven Anmerkungen zum theoretischen Teil dieser Arbeit.

Weiteren Personen, denen mein Dank für das sicherlich nicht immer angenehme Lesen und Kommentieren dieser Arbeit gilt, sind zudem Ann-Sophie Engels, Franziska Fahrbach, sowie Annika Zettl.

Besonderen Dank möchte ich nochmals Prof. Dr. Wolf J. Schünemann, sowie den weiteren HerausgeberInnen Prof. Dr. Jeanette Hofmann, Prof. Dr. Claudia Ritzi und Prof. Dr. Norbert Kersting dafür aussprechen, dass sie mein Buch in ihre Reihe *Politik in der digitalen Gesellschaft* aufgenommen haben.

Am meisten Geduld aufgebracht und Optimismus versprüht während der Entstehungszeit dieses Buches hat jedoch neben meiner Familie besonders meine Frau Christine Schabath, ohne die ich meine Promotion nicht halb so gut überstanden hätte.

März 2023

Abkürzungsverzeichnis

AIVD	Algemene Inlichtingen- en Veiligheidsdienst (niederländischer In- und Auslandsgeheimdienst)
AMAN	Israeli Directorate of Military Intelligence
APEC	Asia-Pacific Economic Cooperation
APT	Advanced Persistent Threat
ASEAN	Association of Southeast Asian Nations
AU	Afrikanische Union
AV	Abhängige Variable
BIP	Bruttoinlandsprodukt
BIR	Bureau of Intelligence and Research (USA)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CCDI	Central Commission for Discipline Inspection (VR China)
CEO	Chief Executive Officer
CFR	Council on Foreign Relations
CIA	Central Intelligence Agency (USA)
CIA	Confidentiality, Integrity, Availability (CIA-Triade der Informationssicherheit)
CISA	Cybersecurity and Infrastructure Security Agency
CNITSEC	China Information Technology Security Center
CNNVD	Chinese National Vulnerability Database
COC	Code of Conduct
CPO	Causal-Process Observations
CSIS	Center for Strategic and International Studies
DCID	Dyadic Cyber Incident and Dispute Datasets
DHS	Department of Homeland Security (USA)
DIA	Defense Intelligence Agency (USA)
DNC	Democratic National Committee (USA)
DoD	Department of Defense (USA)
DoJ	Department of Justice (USA)
DoT	Department of Treasury (USA)
DSO	Data-Set Observations

EU	Europäische Union
FAPSI	Federal Agency for Government Communications and Informations (Russland)
FBI	Federal Bureau of Investigation
FDI	Foreign Direct Investment
FSB	Federalnaja sluschba besopasnosti Rossijskoi Federazii (russischer Inlandsgeheimdienst)
GRU	Glawnoje Raswedywatelnoje Uprawlenije (russischer Militärgeheimdienst)
GSD	General Staff Department (VR China)
GSP	Microsoft Government Security Program
GTsST	GRU's Main Centre for Special Technologies
GUS	Gemeinschaft unabhängiger Staaten
HD-CY.CON	Heidelberg Cyber Conflict Dataset
HIIK	Heidelberger Institut für Internationale Konfliktforschung
HUMINT	Human Intelligence
IAEA	International Atomic Energy Agency
ICD	Intelligence-Community Directive (USA)
ICS	Industrial Control Systems
ICT	Information and Communication Technology
IDF	Israeli Defense Forces
IMINT	Imagery Intelligence
INCB	Israel National Cyber Bureau
INEW	Integrated Network Electronic Warfare
IO	Internationale Organisation
IOC	Indicator of Compromise
IRG	Iranische Revolutionsgarden
ISP	Internet Service Provider
IV	Intervenierende Variable
IVEP	International Vulnerabilities Equities Process
JCPOA	Joint Comprehensive Plan of Action
JSSD	Jiangsu Ministry of State Security (VR China)
KPC	Kommunistische Partei Chinas
KV	Konditionierende Variable
MAPP	Microsoft Active Protection Program
MOSSAD	Israeli Secret Intelligence Service
MPS	Ministry of Public Security (VR China)
MSP	Managed Service Provider
MSS	Ministry of State Security (VR China)
NATO	North Atlantic Treaty Organization
NCPI	National Cyber Power Index
NCSA	National Cyber Security Authority (Israel)
NCSC	National Cyber Security Centre (Großbritannien)
NGO	Non-Governmental Organization
NSA	National Security Agency (USA)

OBOR	One Belt, One Road Initiative (VR China)
ODNI	Office of the Director of National Intelligence (USA)
ONSI	Office of National Security Intelligence (USA)
OPCW	Organisation for the Prohibition of Chemical Weapons
OSF	Open Society Foundation
PDD	Presidential Decision Directive (USA)
PLA	People's Liberation Army (VR China)
PNAC	Project for the New American Century
RBN	Russian Business Network
RISS	Russian Institute for Strategic Studies
SBU	Sluschba bespeky Ukrajiny (Inlandsgeheimdienst der Ukraine)
SCADA	Supervisory Control and Data Acquisition
SFC	Structured Focussed Comparison
SHABAK	Israeli General Security Service
SIGINT	Signals Intelligence
SORM	System of Operational-Investigatory Measures (Russland)
SOZ	Shanghaier Organisation für Zusammenarbeit
SSF	Strategic Support Forces (VR China)
SWR	Sluschba wneschnei raswedki (russischer Auslandsnachrichtendienst)
TPP	Freihandelsabkommen Trans-Pacific Partnership
TTP	Tactics, Techniques and Procedures
UdSSR	Union der Sozialistischen Sowjetrepubliken
UN/UNO	Vereinte Nationen
USA	United States of America
US CYCOM	US Cyber Command
UV	Unabhängige Variable
VEP	Vulnerabilities Equities Process
WHO	Weltgesundheitsorganisation
WTO	Welthandelsorganisation

1. Einleitung: Die Übertragung der Staat-Proxy-Logik auf den Cyberspace

Australischer Verteidigungsminister: »Is this China?«
Chef des Australischen Geheimdiensts (ASD): »A viable possibility, we can't discount al Qaeda, North Korea…«
Australische Justizministerin: »Speculation is no help.«
Chef des Australischen Geheimdiensts (ASD): »It could be homegrown. Though they haven't tripped alerts. We have had no warning.«
Australischer Verteidigungsminister:
»For christ's sake people, we know who it is!«.
Transkription aus der Streaming-Serie »Secret City«, Staffel 1, Folge 4

1.1 Autokratien und Demokratien: unterschiedliche Proxy-Nutzung im Cyberspace?

Der hier vorgestellte Dialog entstammt zwar einer fiktiven Serie, könnte sich jedoch so oder in ähnlicher Form auch in der Realität in einem nationalen ›Situation-Room‹ abspielen. In der Serienepisode hatten unbekannte Hacker das Flugkommunikationssystem Australiens und somit Teile der kritischen Infrastrukturen des Landes unter ihre Kontrolle gebracht. Wie der Dialog verdeutlicht, vermuteten die Verantwortlichen zwar einen politischen Rivalen, konkret die Volksrepublik (VR) China, als Urheber, konnten dies jedoch noch nicht mit entsprechenden Beweisen belegen. Gleichzeitig verwies der Geheimdienstchef auf die Möglichkeit alternativer Attributionen in Richtung nichtstaatlicher AkteurInnen. Die Frage der Attribution erlangte in den letzten zehn Jahren Bedeutung im öffentlichen, politischen sowie wissenschaftlichen Diskurs über Cyberkonflikte. Verstärkt wird das dabei thematisierte ›Attributionsproblem‹ nicht nur durch die

bereits bestehenden technischen Herausforderungen des dezentralen Internets als Konfliktaustragungsraum, sondern auch durch den Einsatz von StellvertreterInnen für die Durchführung offensiver Cyberoperationen. In der Geschichte dienten nichtstaatliche AkteurInnen Staaten im Rahmen traditioneller Konflikte bereits in vielen Fällen als nützliche Partner, Erfüllungsgehilfen oder auch Sündenböcke. Gerade zu Zeiten des Kalten Krieges kam es sowohl auf Seiten der USA als auch der Sowjetunion (UdSSR) zur unterschiedlichen Instrumentalisierung dieser *Proxys* im Rahmen der sog. ›Stellvertreterkriege‹. Dabei unterstützten die USA etwa die Contra-Rebellen in Nicaragua (Klare 1989), die UdSSR sponserten die Palästinensische Befreiungsorganisation (PLO) (Spiegel 1983, S. 51). Somit mischten sich die beiden Großmächte in bereits bestehende Konflikte außerhalb ihres Staatsgebietes ein, indem sie eine der nationalen Konfliktparteien materiell und/oder immateriell unterstützten. Durch diese Form der ›indirekten Intervention‹ (Mumford 2013) konnten die Staaten ihre Interessen im Rahmen der Konflikte verfolgen, ohne dabei zu direkten Konfliktparteien zu werden und entsprechende politische und ökonomische Kosten tragen zu müssen. Da sowohl der unterstützende Staat als auch der Proxy ihre bestehende Beziehung öffentlich nicht eingestehen, gelingt es insbesondere dem staatlichen ›Benefactor‹ (Wohltäter/Sponsor), die sog. ›Plausible Deniability‹ (plausible Bestreitbarkeit) über die eigene Involvierung in den Konflikt zu bewahren. Außer aufgrund der reinen Kostenersparnis sowie einer niedrigeren Eskalationsgefahr lohnte sich eine Unterstützung einheimischer KonfliktakteurInnen aus Sicht der Staaten ferner, da diese über einen ›Local Advantage‹ im Konfliktaustrag verfügten, z.B. die geografischen Gegebenheiten des Landes besser kannten, als dies den eigenen Militärtruppen im Rahmen einer direkten Intervention hätte möglich sein können (vgl. Mumford 2013).

In der neueren Historie der wissenschaftlichen und öffentlichen Verwendung des Proxy-Begriffes wird diesem immer häufiger das Präfix ›Cyber‹ vorangestellt. Eine Google-(Scholar)-Suche des Begriffes *Cyberproxy* fördert dabei jedoch im Gegensatz zu den für die USA nachgewiesenen Beziehungen zu konventionellen Proxys fast ausschließlich Berichterstattungen über autokratische Stellvertreternutzungen im Cyberspace zu Tage. Wie lässt sich dieser Befund erklären? Sind Demokratien im Cyberspace schlicht nicht auf die Hilfe privater AkteurInnen zur Durchführung offensiver Operationen angewiesen oder verzichten sie gar regelmäßig auf eigene Cyberangriffe? Um die These demokratischer Zurückhaltung im Cyberspace in einem ersten Schritt zu testen, wird in dieser Arbeit im Zuge der empirischen Analyse auf einen umfassenden Cyberkonfliktdatensatz zurückgegriffen. Der Vergleich zwischen autokratischem und demokratischem Cyberkonfliktaustrag stellt jedoch nur eine notwendige Vorstufe dar, um die im Zentrum der Arbeit stehenden Proxys im Cyberspace regimetypenspezifisch untersuchen zu können. Dabei soll die Frage beantwortet werden, ob nichtstaatliche AkteurInnen auch für Demokratien im Cyberspace als Proxys fungieren können, jedoch nicht in der Rolle des Angreifers, sondern des Opfers von Cyberoperationen. Die zentralen Forschungsfragen lauten somit:

Welche Arten von Proxys im Cyberspace nutzen Autokratien und Demokratien trotz eigener, technischer Kapazitäten? Welche Funktionen übernehmen diese und unter welchen Bedingungen?

Bearbeitet werden diese Fragen aus der Perspektive des neuen Liberalismus nach Andrew Moravcsik: Zum einen erlaubt der liberale Theorieansatz die Inklusion nichtstaatlicher AkteurInnen auf beiden Seiten der Konfliktdyade, zum anderen kann durch

das Theoriemodell Moravcsiks der Einfluss von Präferenzordnungen auf unterschiedlichen Ebenen untersucht werden. So könnte eine ausschließliche Fokussierung auf sicherheitspolitische oder wirtschaftliche Präferenzen der Staaten die große Varianz der Interessen, die durch den Einsatz unterschiedlicher Proxys im Rahmen unterschiedlicher Cyberoperationen verfolgt werden sollen, nicht adäquat erfassen.

Ein Blick in die öffentliche Berichterstattung im Rahmen von Cyberoperationen[1] liefert für eine stärker defensiv geprägte Staat-Proxy-Beziehung auf demokratischer Seite erste Indizien: So dominieren vor allem private IT-Unternehmen den Detektions- und Attributionsdiskurs im Rahmen von Cyberoperationen, wie auch die spätere Analyse zeigen wird. Privatwirtschaftliche AkteurInnen decken Cyberoperationen zwischen Staaten und deren Proxys, jedoch auch nichtstaatlichen AkteurInnen, nicht nur häufig auf, sondern attribuieren diese zudem auch in immer mehr Fällen, oftmals in Richtung staatlicher UrheberInnen (vgl. Romanosky und Boudreaux 2021). Aus dieser Beobachtung wird in der Arbeit das Argument entwickelt, dass diese stellvertretende Attribution als defensive Funktion demokratischer IT-Unternehmen als Proxys im Rahmen von Cyberkonflikten gewertet werden sollte, im Gegensatz zu den offensiven Cyberoperationen autokratischer StellvertreterInnen.

Aus liberaler Theorieperspektive werden hierfür unterschiedliche Erklärungsansätze diskutiert und darauf aufbauend wird ein eigenes Erklärungsmodell entwickelt. Dieses soll es ermöglichen, nicht nur das empirische Puzzle bezüglich der Autokratie-Demokratie-Unterscheidung, sondern auch innerhalb der Lager zu beobachtende Varianzen hinsichtlich der offensiven (Hacking) oder defensiven (Attribution) Cyberproxynutzung erklären zu können. Die drei Spielarten des Liberalismus von Andrew Moravcsik dienen dabei als theoretische Erklärungsansätze, die es auf die Staat-Proxy-Beziehung im Cyberspace zu übertragen gilt. Dabei werden domestische Präferenzbildungsprozesse das Kernstück der Analyse darstellen, die den autokratischen und demokratischen Entscheidungsprozess auf außenpolitischer Ebene entscheidend prägen. Der unterschiedliche Herrschaftszugang bestimmter domestischer Gruppen dient als eine zentrale Erklärungsvariable für die überwiegend offensive vs. defensive Cyberproxynutzung der beiden Regimetypen.[2]

Mithilfe jeweils zweier Fallstudien (Russland und China sowie USA und Israel) werden Unterschiede der Cyberproxynutzung zwischen und innerhalb der beiden Regimetypenkategorien konzeptualisiert und aus liberaler Sicht erklärt.[3] Grundlage für die empirische Analyse der jeweiligen Cyberproxystrategien ist dabei ein umfassender Cyberkonfliktdatensatz (HD-CY.CON), der es erlaubt, im Gegensatz zu den bislang

---

1 Der Begriff ›Cyberoperationen‹ wird verwendet, um sowohl ›Cyber Network Exploitations‹, die vor allem Spionagetätigkeiten umfassen, als auch disruptivere Operationen, sog. ›Cyber Network Attacks‹, zu inkludieren (vgl. Lin 2010, S. 63).

2 Regime werden definiert als *»a set of rules that identifies: who has access to power; who is allowed to select the government; and under what conditions and limitations authority is exercised«* (Kailitz 2013, S. 39).

3 Ein »Fall« bedeutet im Rahmen dieser Arbeit die Cyberproxy-Nutzung eines Landes im Untersuchungszeitraum, entsprechend des theoretischen Verständnisses *»of a case to include many observations on the same variable«* (Levy 2008, S. 3).

vorherrschenden quantitativen Einzelfall- oder Small-N-Studien die theoretischen Annahmen auf einer möglichst breiten quantitativen Datenbasis überprüfen zu können.[4] Somit wird mit dieser Arbeit auch auf methodologischer Ebene ein Beitrag zur weitgehend noch in ihren Anfängen befindlichen Cyberkonfliktforschung geleistet, indem erstmals auf Grundlage einer umfassenden Datenbasis Large-N-Untersuchungen von Cyberoperationen angestellt und diese gleichzeitig im Rahmen eines Mixed-Methods-Designs auch für qualitative Analysemethoden nutzbar gemacht werden. Konzeptionell wird die Frage nach regimetypenspezifischen Charakteristika und deren Auswirkungen im vernetzten und interdependenten Konfliktaustragungsraum des Cyberspace erstmals direkt an staatliche Cyberkonfliktstrategien angebunden. Durch den liberalen Theorieansatz kann zudem zwischen stärker institutionell verorteten Aspekten der domestischen Interessensvertretung sowie deren tatsächlichen Inhalten auf unterschiedlichen Ebenen differenziert werden. Somit sollen auch potenzielle Gemeinsamkeiten unterschiedlicher Regimetypen aufgrund konvergierender Präferenzkonstellationen in einem Bereich identifiziert werden können. Insgesamt wird in der Arbeit jedoch von größeren Präferenzinkompatibilitäten zwischen Autokratien und Demokratien ausgegangen, was als zentrale Erklärung für die interdependente Proxy-Nutzung beider Regimetypen im Rahmen von Cyberoperationen angeführt wird.

Somit ergibt sich für die vorliegende Arbeit sowohl eine wissenschaftliche als auch eine gesellschaftliche Relevanz (vgl. King et al. 1994, S. 15): Zum einen wird durch die Entwicklung eines liberalen Erklärungsmodells unterschiedlicher Staat-Proxy-Beziehungen auf der Grundlage eines umfassenden Cyberkonfliktdatensatzes der Dialog zwischen Theorien und Daten über den aktuellen Forschungsstand hinaus vorangetrieben. Die Arbeit ist somit explorativ, da ein neuer Theorieansatz für ein noch untererforschtes Forschungsfeld entwickelt und empirisch getestet wird. Die Arbeit ist jedoch auch in Teilen theorietestend, da im Zuge des Schlusskapitels bereits bestehende Theorien als alternative Erklärungsansätze für die empirischen Befunde diskutiert werden sollen. Indem das Proxy-Modell auf hierfür bislang noch nicht prädestinierte AkteurInnen, die IT-Unternehmen demokratischer Länder, übertragen wird, erfolgt zudem die Dekontextualisierung eines bestehenden Theoriemodells. Dies geschieht sowohl hinsichtlich der Art der Handlungen, die seitens des Proxys stellvertretend für den Staat vorgenommen werden, als auch hinsichtlich des Konfliktaustragungsraumes. Bislang konzentrierte sich die politikwissenschaftliche Proxy-Forschung auf ›Proxy-Wars‹ im konventionellen Bereich und verortete Proxys somit stets als gewaltsame AkteurInnen im Rahmen militärischer Konflikte (vgl. Rauta 2021). Wie in der vorliegenden Arbeit gezeigt werden soll, können Proxys insbesondere im Rahmen bislang noch weitgehend gewaltloser Cyberkonflikte, die zudem Teil komplexer politischer und wirtschaftlicher Interdependenzen sind, auch demokratischen Staaten durch deren defensive Funktionserfüllung Kosten auf nationaler sowie internationaler Ebene ersparen. Liberal formuliert handelt es sich hierbei um die Manipulation bestehender

4 Diese stärkere Datenorientierung forderten auch Brandon Valeriano und Ryan C. Maness in einem 2018 veröffentlichten Artikel zu den methodischen Herausforderungen der empirischen Cyberkonfliktforschung.

Interdependenzverhältnisse nach innen und außen, die durch den Einsatz von Proxys erreicht werden soll.

Gesellschaftliche Relevanz entfaltet die Arbeit dagegen in folgender Hinsicht (vgl. Gschwend und Schimmelfennig 2007, S. 15): Erstens wird ein zunehmend sekuritisiertes Untersuchungsfeld bearbeitet. Sowohl politische als auch privatwirtschaftliche AkteurInnen zeigen ein stetig steigendes Interesse daran, durch teilweise unverhältnismäßige Formulierungen den Cyberspace als ›Fifth Domain‹ zu kennzeichnen.[5] PolitikerInnen bietet dies die Chance, steigende Sicherheitsbudgets im Cyberspace sowie in Teilen auch kontroverse Eingriffe in die individuelle Privatsphäre eigener und fremder BürgerInnen zu rechtfertigen. Für IT-Unternehmen lohnt es sich, die Anzahl und Schwere stattfindender Cyberangriffe ebenfalls permanent zu betonen, da sie es sind, die mit ihren Produkten Schutz vor den stetig steigenden Gefahren im Cyberspace versprechen. Indem somit eine möglichst breite Datenbasis über (öffentlich bekannte) Cyberoperationen und deren Intensität vorgestellt und analysiert wird, kann die tatsächliche Cyberkonfliktlandschaft besser als auf Grundlage bloßer Einzelfallstudien bewertet werden. Trotz der genannten Sekuritisierung ist unbestritten, dass der potenzielle Angriffsvektor im Cyberspace zunehmend steigt, sei es durch das Internet of Things, die Integration künstlicher Intelligenz in Produkten des privaten sowie öffentlichen Sektors sowie sonstige Digitalisierungsmaßnahmen. Der Cyberspace und dessen Verregelung bzw. der Schutz öffentlicher Systeme, allen voran kritischer Infrastrukturen, stellen somit hohe öffentliche Güter dar, die es vor dieser steigenden Gefahr zu schützen gilt, bei gleichzeitig notwendiger, zielspezifischer Risikoabschätzung. Zweitens kann die vorliegende Arbeit auch das Problemverständnis politischer EntscheidungsträgerInnen im Umgang mit ausländischen HackerInnen stärken. Denn nur, wenn sie ein entsprechendes Verständnis darüber entwickeln, welcher Art die Beziehung zwischen nichtstaatlichen AkteurInnen als Proxys (autokratischer) Staaten sein kann und in den jeweiligen Fällen konkret ist, können auch effektive politische Reaktionsoptionen entwickelt werden. Die Motivlage des Staates sowie des Proxys für die Aufnahme der Beziehung zu kennen, ist hierfür genauso wichtig, wie ein umfassendes Verständnis für die jeweiligen Handlungsrestriktionen dieser AkteurInnen zu entwickeln.

1.2 Bisheriger Forschungsstand zu Proxys im Cyberspace

Damit das avisierte Erklärungsmodell im Kontext bereits existierender Forschungsarbeiten zum Thema der staatlichen (Cyber-)Proxy-Nutzung situiert werden kann (George und Bennett 2005, S. 70), müssen diese zunächst beschrieben werden. Somit können notwendige Modifizierungen etablierter Konzepte begründet werden. Nachfolgend wird zunächst auf die unterschiedlichen Definitionen des Konzepts des Cyberproxys in relevanten Forschungsarbeiten eingegangen. Anschließend wird der Forschungsstand zur Nutzung dieser Cyberproxys in Demokratien und Autokratien näher beleuchtet.

5 Beispiele hierfür sind die Analogien ›Cyber Pearl Harbor‹, ›Cyber-Armageddon‹ oder auch ›World War C‹.

Das Konzept des ›Cyberproxy‹ fungiert generell als Oberkategorie für verschiedene Akteurskategorien. In der Forschungsliteratur wurden bislang hauptsächlich folgende Akteursgruppen als potenzielle TrägerInnen der Proxy-Rolle im Rahmen von Cyberoperationen identifiziert, die entweder durch militärische oder zivilgeheimdienstliche AkteurInnen an den jeweiligen Staat angebunden sein können:

- *Cybermilizen:* Der Term ›*Cybermilitia*‹ diente bislang als eine Art Sammelbegriff für staatlich gesponserte (Applegate 2011, S. 18), andererseits jedoch auch aus eigenen Stücken agierende, patriotisch gesinnte Zusammenschlüsse organisierter HackerInnen oder auch CybersicherheitsexpertInnen (Dudney 2011), die ad hoc oder permanent geformt werden (Ottis 2010, S. 233). Die jeweiligen Fähigkeiten hängen dabei von den individuellen Kenntnissen und Kapazitäten der Gruppenmitglieder ab (Sigholm 2013, S. 11). Anwendung fand das Konzept bislang vor allem für die Volksrepublik China (Harris 2008; Krekel 2009; Dudney 2011).[6]
- *Patriotische HackerInnen:* Cybermilizen und patriotische HackerInnen unterscheiden sich hauptsächlich in ihrem jeweiligen Organisationsgrad (vgl. Applegate 2011; Dudney 2011). Bei Letzteren besteht keine Hierarchie oder regelmäßige Vernetzung zwischen den einzelnen HackerInnen, gemeinsam haben sie jedoch ihre patriotische Gesinnung, der sie überwiegend mithilfe technisch anspruchsloserer Angriffe wie *Defacement*- und DDoS-Attacken Ausdruck verleihen (Romagna und van den Hout 2017; Whyte 2018).
- In Abgrenzung zum Konzept der HacktivistInnen sticht bei patriotischen HackerInnen deren nationalistische, regierungsaffine Position heraus. Erstere agieren dagegen oftmals in Opposition zum jeweiligen Staat oder verfolgen eine bewusst transnationale, kosmopolitische Agenda (Dahan 2013, S. 53–54).
- *Cyberkriminelle:* Für das Cyberproxykonzept insgesamt gewannen auch Cyberkriminelle und deren Verbindungen zum jeweiligen Heimatstaat in den letzten Jahren zunehmend an Bedeutung. Die schwierige Differenzierung zwischen »*Cyber crime, cyber terrorism and cyber warfare*« (Klimburg 2011, S. 41) rückte dabei besonders in den wissenschaftlichen Fokus. Ähnlich wie bei der Unterscheidung zwischen lose affiliierten patriotischen HackerInnen und organisierten Cybermilizen wurden auch bei Cyberkriminellen verschiedene Organisations- und Hierarchieformen unterschieden und zudem in Bezug zu den oftmals als AuftraggeberInnen fungierenden staatlichen AkteurInnen gesetzt (Broadhurst et al. 2014). Staatlich zumindest geduldete Cyberkriminelle erfahren seit den russischen Ransomware-Operationen gegen US-Infrastrukturen 2021 wieder verstärkt politische Aufmerksamkeit (Wilkie 2021).
- *Private Military Security Contractors (PMSCs):* In der Forschungsliteratur werden zudem PMSCs häufig als stellvertretende Einheiten vor allem demokratischer Staaten behandelt, denen der Einsatz von Gewalt nur zur Verteidigung erlaubt ist und die vor allem logistische Unterstützungsleistungen erfüllen. Deren teilweise unrechtmäßige Gewaltanwendung im Rahmen bewaffneter Konflikte wurde jedoch im Sinne der Schwächung des demokratischen Gewaltmonopols durch Vertragsnehmer wie das US-Unternehmen *Blackwater* zunehmend kritisch diskutiert (Carmola 2010; Nevers

6 Im weiteren Verlauf wird die Volksrepublik China auch als ›VR China‹ oder nur ›China‹ bezeichnet.

2016). Über autokratische PMSCs im Allgemeinen sowie im Rahmen von Cyberkonflikten im Besonderen wurde bislang weitaus weniger publiziert. Russland kann dabei für die Ukraine- und Syrienkriege noch als Ausnahme gelten (u.a. Fainberg 2017; Sukhankin 2018; Marten 2019). Im Fokus der Aufmerksamkeit standen dabei die »*RSB-Group*« (Østensen und Bukkvoll 2018, S. 23) sowie die bekannteste russische PMSC »*Wagner*«. Letztere besitzt laut öffentlichen Berichten eine im Gegensatz zu demokratischen PMSCs größere ideologische Bindung zum russischen Heimatstaat (Bukkvoll und Østensen 2020, S. 2–3). Hinsichtlich einer Cyberproxy-Rollenübernahme könnte diese Regimetypenunterscheidung für den Motivationsfaktor der *Ideologie* somit von zunehmender Bedeutung sein.

Proxys wurden im Cyberspace bislang fast ausschließlich als offensiv agierende, Cyberattacken ausführende AkteurInnen behandelt (Schmitt und Vihul 2014; Maurer 2016; Maurer 2018a; Maurer 2018b; Borghard und Lonergan 2016; Canfil 2016). In seiner Arbeit von 2016 verweist Tim Maurer darauf, dass selbst auf völkerrechtlicher Ebene jedoch noch keine umfassende Definition des Begriffes ›Cyberproxy‹ existiere, auch wenn dieser dort bereits verwendet wurde (in den UNGGE Reports 2013 und 2015). Zudem sei dessen Übersetzung in nicht englischsprachige Kontexte ebenfalls erschwert und nicht weiter spezifiziert (2016, S. 384). In der Folge arbeitete Maurer daher eine Art kleinsten gemeinsamen Nenner bezüglich des Terminus heraus: Damit werde überwiegend auf die Beziehung zwischen einem nichtstaatlichen Akteur (Proxy/Agent) und einem Staat (Prinzipal/Benefactor) angespielt. Diese Akteurskonstellation sei empirisch besonders relevant und somit auch die primär untersuchungswürdige (2016, S. 383). Auch in den Arbeiten von Schmitt und Vihul 2014 sowie Borghard und Lonergan 2016 zur Thematik, die sich ebenfalls an der Principal-Agent-Theorie orientierten, spiegelt sich dieser Konsens wider.

2016 widmete sich Maurer zudem Fragen der rechtlichen Verantwortungszuweisung von Cyberproxy-Aktivitäten: Wann kann ein Staat überhaupt für die Handlungen seines angeblichen Proxys verantwortlich gemacht werden? In diesem Kontext diskutierte er das Konzept der ›Due Diligence‹ (Sorgfaltsverantwortung) und welche Erwartungen an deren Anwendung im Cyberspace realistischerweise geknüpft werden könnten (S. 384).

Im Gegensatz zu diesen primär theoretischen Überlegungen bearbeitete Maurer in seinem Buch »Cyber-Mercenaries« aus 2018 stärker empirische Beispiele offensiver Cyberproxy-Nutzung (2018a, S. 7). Ein Cyberproxy ist nach Maurer ein »*intermediary that conducts or directly contributes to an offensive action that is enabled knowingly, actively or passively, by a beneficiary*« (2018a, S. 31). Dabei bezieht er sich ausschließlich auf AkteurInnen als Proxys, die zu autonomer Entscheidungsfindung befähigt sind, im Gegensatz zu ebenfalls oft als ›Proxys‹ betitelten technischen Hilfsmitteln (2018a, S. 31). Maurer unterscheidet grundlegend drei Formen der Staat-Proxy-Beziehung: ›Delegation‹ beschreibt dabei die engste Anbindung und damit auch das größtmögliche Maß an Kontrolle über einen nichtstaatlichen Akteur im Cyberspace. Als empirisches Fallbeispiel rekurriert der Autor hierbei auf die USA und deren Nutzung von privaten Sicherheitsfirmen zur Planung und Vorbereitung von Cyberangriffen. In der vorliegenden Arbeit wird eine solche Tätigkeit jedoch aus der Cyberproxy-Definition ausgeschlossen, da hierbei der Angriff final immer noch von einer staatlichen Stelle selbst ausgeführt wird und die üblicherweise

angestrebte Plausible Deniability nicht das primäre Ziel der Einbindung dieser privaten AkteurInnen in die sog. »Cyber-Kill-Chain« (Lockheed Martin 2020) sein kann.[7] Dies ist besonders für die Spionage- und Überwachungstätigkeiten der National Security Agency (NSA) der USA von Bedeutung: Die Enthüllungen Edward Snowdens legten offen, welche Rolle private Dienstleister wie Booz Allen Hamilton oder Lockheed Martin bei der Geheimhaltung der Handlungen an sich spielten, indem deren technische Fähigkeiten zur Planung und Vorbereitung seitens der NSA unter einem hohen Maß an »Operational Security« genutzt wurden. Somit stand hier die Verschleierung der eigenen, liberal-demokratischen Prinzipien widersprechenden Praktiken im Vordergrund, gerechtfertigt vor allem durch das in US-Geheimdienstkreisen etablierte Post-9/11-Sekuritisierungsnarrativ NOBUS (»nobody but us«; Perlroth 2021).[8] Dass speziell in demokratischen Staaten die Beauftragung privater Unternehmen in der Regel durch öffentlich sichtbare Verträge formalisiert wird, spricht ebenfalls gegen die Anwendbarkeit des zentralen Proxy-Motivs der plausiblen Bestreitbarkeit.[9] In demokratischen Staaten werden SubunternehmerInnen vor allem zum Zwecke der Geheimhaltung des Angriffes benutzt. Die Geheimhaltung der Beziehung zum Proxy selbst ist dagegen kein zentrales Ziel dieser Interaktion. Durch öffentliche Haushaltsdebatten, Verträge mit den jeweiligen Firmen sowie demokratische Geheimdienstausschüsse erfolgt in diesen Staaten lediglich eine operative, im Cyberraum oftmals notwendige Geheimhaltung der Angriffspläne. Deren Planung und Durchführung werden dabei durch die entsprechend demokratisch legitimierten Institutionen begleitet und auch kontrolliert. Somit soll sichergestellt werden, dass das Gewaltmonopol im Cyberspace immer noch in den Händen des Staates liegt, gleichzeitig jedoch die eigenen Cyberkapazitäten im Rahmen offensiver Operationen trotz demokratischer Beschränkungen und Kontrollinstanzen effektiv arbeiten können. Aus diesem Grunde können beispielsweise die Geheimdienste sowie die mit ihrer Kontrolle betrauten Ausschüsse nie vollständig öffentlich agieren. Dennoch sollen solch institutionelle Checks and Balances die staatliche Hoheit im eigenen Cyberkonfliktaustrag gewährleisten. Für das Beispiel der USA bedeutet dies jedoch, dass die Geheimhaltung der NSA-Überwachung primär nach innen gerichtet war, um eben jene institutionalisierten Kontrollmechanismen umgehen zu können. Hinzu kommt, dass hierdurch ebenso die illegitime Überwachung eigener BürgerInnen geheim gehalten werden sollte. Zwar war diese aus Sicht der US-Regierung zwingend notwendig, um in Folge des 11. Septembers der Infiltration der USA durch potenzielle TerroristInnen entgegen zu wirken. Gleichzeitig

7 Auch aus völkerrechtlicher Sicht werden PMSCs, welche *nicht* in die bewaffneten Streitkräfte durch konfliktive Tätigkeiten integriert sind, als weniger salient bezüglich der Konfliktentwicklung angesehen, da diese wie unbeteiligte ZivilistInnen auch, als NichtkombattantInnen eingestuft werden (Melzer 2008, S. 39). Das Prinzip kann somit auch für das bloße Schreiben eines Malware-Codes, ohne dessen tatsächlicher Ausführung, seitens des privaten Auftragnehmers angewandt werden (Crawford 2013, S. 16).

8 »Nobody but us« sollte aus Sicht der US-Geheimdienste z.B. dazu im Stande und auch legitimiert sein, entdeckte Sicherheitslücken in Netzwerken für Cyberoperationen auszunutzen.

9 So ist beispielsweise für den erwähnten PMC Blackwater bekannt, dass dieser im Zuge seines Einsatzes im Irakkrieg von 2000 bis 2007 öffentliche Aufträge der USA im Wert von mehr als einer Milliarde Dollar erhalten hat (U.S. Government 2007, S. 2).

zeigt die jahrelange Verschleierung dieser Praxis die asymmetrische Verwundbarkeitssituation in der sich Demokratien gegenüber Autokratien und Terrorgruppen befinden. So schützen die eigenen Gesetze nicht nur die eigenen BürgerInnen vor Übergriffen staatlicher Behörden, sondern eben auch ausländische Akteure mit schädigenden Absichten.

Der zweite Beziehungstypus, den Maurer vorschlägt, sieht dagegen eine losere Staat-Proxy-Beziehung vor. Im Rahmen der ›Orchestration‹ wird der Proxy weniger stark durch den ›Beneficiary"[10] kontrolliert. So kann der Stellvertreter spezifische Zielsysteme und Angriffsmethoden selbst bestimmen. Entscheidend ist jedoch die üblicherweise bestehende ideologische Übereinstimmung zwischen den beiden AkteurInnen (Maurer 2018a, S. 12). Entgegen dem Titel des Buches weicht Maurer hier somit von der rein finanziellen Motivlage der ›Mercenaries‹ (Söldner) ab. Er demonstriert diese Form der Kooperation anhand der Beispiele Iran und Syrien. Letzteres Regime unterstütze die sog. Syrian Electronic Army Berichten zufolge auf ideologischer Ebene, aber anscheinend auch durch die Bereitstellung von Infrastruktur (Al-Rawi und Ahmed K. 2014). Die dritte Beziehungsform des ›Sanctionings‹ bezieht sich auf die passivste Rolle des Prinzipals und sieht diesen lediglich in einer Art ›gewährenden‹ Rolle vor, der ›ein Auge zudrückt‹, wenn der Proxy beispielsweise vom eigenen Staatsterritorium aus eine Cyberattacke auf einen anderen Staat ausübt. Zwar ordnet der Staat diese Attacke nicht an und unterstützt sie auch nicht materiell, er unterbindet sie jedoch auch nicht, wenn sie mit seinen eigenen Interessen übereinstimmt (Maurer 2018a, S. 20). Hierfür wählte Maurer Russland als Fallbeispiel. Ein potenzieller Wandel in der vorherrschenden Staat-Proxy-Beziehung wird darüber hinaus am Beispiel Chinas demonstriert: Laut Maurer verdrängte hier im Laufe der Zeit der Typus der Delegation das zuvor vorherrschende Beziehungsarrangement des Sanctionings.

In ihrer Arbeit aus 2016 verweisen Erica Borghard und Shawn Lonergan ebenfalls auf die Unterscheidung zwischen den Konzepten der ›Mercenaries‹ sowie der ›Proxys‹ und fügen das Konzept der ›Alliances‹ hinzu. Alle drei Konzepte werden zur Beschreibung der Beziehungsform zwischen nichtstaatlichen AkteurInnen und Staaten im Cyberspace herangezogen (Borghard und Lonergan 2016, S. 401–402). Aus Sicht der AutorInnen eignet sich der Terminus des Proxys für eine sinnvolle Beschreibung dieser Beziehung jedoch am besten: ›Allianz‹ sei keine adäquate Wahl, da hiermit meist zwischenstaatliche, durch öffentlich einsehbare Verträge geschlossene Bündnisse beschrieben werden (2016, S. 402). Der Begriff ›Mercenary‹ sei ebenfalls ungeeignet, um das ganze Spektrum an möglichen Beziehungsformen zwischen nichtstaatlichen AkteurInnen und Staaten zu erfassen, da Söldnern seitens der Genfer Konvention (Artikel 47(2)) eine ausschließlich auf finanziellen Gewinn ausgerichtete Motivation zugesprochen wird, sie keine beteiligte Partei des Konfliktes sind, an dem sie teilnehmen, und ebenfalls eine Art öffentliche Beziehungsform darstellen (Borghard und Lonergan 2016, S. 403).

10 Maurer verwendet den Begriff ›beneficiary‹ anstelle von ›principal‹, um aufzuzeigen, dass das Spektrum an möglichen Staat-Proxy-Beziehungen sehr viel weiter gespannt ist, als sie von traditionellen Principal-Agent-Ansätzen dargestellt wird. Somit könne die Bandbreite zwischen ›principal‹ (delegation), ›orchestrator‹ (orchestration) sowie die Rolle des Staates beim ›sanctioning‹ in einem Begriff vereint werden (Maurer 2018a, S. 21).

In der vorliegenden Arbeit wird der Argumentation von Borghard und Lonergan gefolgt, weshalb für eine möglichst tragfähige und inklusive Analyse der möglichen Beziehungsformen zwischen nichtstaatlichen und staatlichen AkteurInnen im Cyberspace das Konzept des Proxys das geeignetste zu sein scheint. Borghard und Lonergan definieren Staat-Proxy-Beziehungen wie folgt: »*A proxy alliance is an agreement between a state and a non-state group that involves the exchange of military resources in furtherance of a political objective*« (2016, S. 404). Somit inkludieren sie die Beziehungsform des Sanctionings aus Maurers Konzept nicht in ihre Analyse, da hierbei kein Transfer materieller bzw. militärischer Ressourcen (auch in Form von Training oder logistischer Unterstützung) vom Staat an den Proxy stattfindet. Ebenso würde die Delegation-Beziehungsform, wie sie Maurer anhand der Kooperation zwischen der US-Regierung und privaten IT-Firmen beschreibt, nicht unter diese Cyberproxy-Definition fallen. Als wichtigsten kleinsten gemeinsamen Nenner stellen Borghard und Lonergan die »*informal, plausibly deniable nature of the relationship*« zwischen Staat und Cyberproxy heraus, die im Falle öffentlich einsehbarer Verträge zwischen IT-Firmen und der US-Regierung nicht gegeben ist (2016, S. 405). In der vorliegenden Arbeit wird die Logik des Sanctionings jedoch im Gegensatz zu den AutorInnen insbesondere in Bezug auf das Attributionsverhalten privater IT-Firmen in Demokratien aufgegriffen. Es wird hierbei von einem indirekteren Delegationsmodus zwischen Staat und Proxy ausgegangen, der ebenfalls lediglich die Tolerierung/passive Ermöglichung der technischen Attributionen bedeuten könnte. Daher wird in der vorliegenden Arbeit die Logik des Sanctionings als potenzielle Staat-Proxy-Beziehungsform inkludiert.

Ferner schließen Borghard und Lonergan Cyberspionage generell aus ihrer Analyse aus, verweisen jedoch selbst auf die Schwierigkeit, isolierte Spionage von Aufklärung zur Vorbereitung einer disruptiveren Cyberattacke aus Sicht des Opfers zu unterscheiden (2016, S. 406). Da Cyberspionage als prävalente Konfliktform im Cyberspace vermutet wird, findet durch deren Inklusion in der vorliegenden Arbeit eine Abgrenzung von den beiden AutorInnen statt.

Als zentrale theoretische Dimensionen verbinden Borghard und Lonergan allianztheoretische Erwägungen mit ihrer Cyberproxy-Definition, indem sie letztere zu internen und externen Sicherheitsdilemmata in Beziehung setzen. Zunächst erstellen sie hierfür eine Proxy-Typologie, worin der Organisationsgrad (individuell/lose vs. organisiert) sowie die jeweilige Motivation (politisch vs. ökonomisch) als zentrale Kategorien verwendet werden (2016, S. 408).[11] Im Rahmen einer zweiten Typologie unterscheiden sie Proxys anhand des jeweiligen Sicherheitsdilemmas, das besonders relevant/präsent ist (extern vs. intern), sowie des jeweils identifizierten, staatlichen Defizits (»Deficit in Capabilities« vs. »Deficit in Willingness«) (Borghard und Lonergan 2016, S. 414). Auf

11 Für den Typ *individuell organisiert* und *ökonomisch motiviert* benennen die AutorInnen jedoch das Beispiel des ILOVEYOU-Wurms aus 2000. Da dem vermeintlichen Täter Onel de Guzman jedoch keine Beziehung/Unterstützung seitens einer Regierung nachgesagt wurde, erfüllt der Fall genau genommen nicht die eigens formulierte Cyberproxy-Definition der AutorInnen.

dieser Grundlage treffen sie sodann Aussagen über die zu erwartenden staatlichen Proxy-Präferenzen.[12]

Neben diesen dominierenden Cyberproxy-Analysen im Sinne offensiv agierender HackerInnengruppierungen untersuchte Florian Egloff in seiner Dissertation zu »Cyber-Privateers & Cyber-Pirates« aus 2018 die Nähe des jeweiligen, nichtstaatlichen Akteurs zum affiliierten Staat.[13] Durch die Verwendung der Seefahrt-Analogie zeigt Egloff auf, in welchen Fällen Staaten versuchen, diese ›*Proximity*‹ in einer gemeinschaftlich genutzten Sphäre zu ihren Gunsten unterschiedlich zu *framen*, wie es auch im transnational funktionierenden Cyberspace der Fall ist (2018, S. 53). Neben den ›Cyber-Privateers‹ und ›Cyber-Pirates‹ untersucht Egloff jedoch auch ›*Mercantile Companies*‹ als nichtstaatliche AkteurInnen mit varianten Beziehungsformen zu staatlichen Stellen. Damit reicht seine Arbeit näher als die meisten anderen im Themenfeld an die in dieser Arbeit konzeptualisierte, primär demokratisch geprägte Proxy-Definition heran. So sieht Egloff in der Zusammenarbeit zwischen US-amerikanischen Technologie-Firmen und der NSA, wie sie 2013 durch Edward Snowden bekannt wurde, ebenfalls eine Form der Kooperation/Interaktion zwischen nichtstaatlichen AkteurInnen und Staaten im Cyberspace.

Da in der Forschung die Beziehung zwischen Staat und Proxy zumeist einseitig konzeptualisiert werde, stelle das Cyberproxy-Konzept für seine eigene Arbeit nur einen unzureichenden Analyserahmen dar, so Egloff (2018, S. 20). Dagegen betonten andere BeobachterInnen im Kontext, dass der Kern einer Staat-Proxy-Beziehung analog zur Prinicipal-Agent-Theorie auch im Cyberspace auf *gegenseitigem* Nutzen beruhe und somit sehr wohl auch in der Lage sei, die unterschiedlichen Motivlagen des nichtstaatlichen Akteurs zu erfassen (z.B. Borghard und Lonergan 2016, S. 405–406). Die in dieser Arbeit vertretene Perspektive stimmt mit dieser zuletzt beschriebenen Ansicht überein.

Weitere Arbeiten, in denen defensivere Funktionen nichtstaatlicher AkteurInnen im Cyberspace unter staatlicher Duldung oder Anleitung thematisiert wurden, sind die Beiträge von Kristen Eichensehr aus den Jahren 2017, 2019 und 2020 sowie die Arbeiten von Romanosky 2017 sowie Romanosky und Boudreaux 2021. Diese deuteten erstmals auf den Mehrwert, aber auch die potenziellen Risiken der von IT-Firmen getätigten Attributionen für demokratische Regierungen hin, auch wenn erstere dabei nicht als Proxys benannt wurden.[14]

---

12 Dabei werden zwei unterschiedliche Staat-Proxy-Beziehungsformen Russlands (einerseits zum Russian Business Network und andererseits zu patriotischen HackerInnen) als Beispiele für sowohl das Wirken des externen, als auch des internen Sicherheitsdilemmas herangezogen. Dies lässt die Frage offen, wann welchem von beiden die größere Wirkmacht seitens des Staates zugesprochen wird und es somit zu unterschiedlichen Proxy-Nutzungsstrategien kommt.

13 Auch Egloff spricht (wie Maurer) nicht ausschließlich von Cyberproxies. Aufgrund der vorgestellten theoretischen Überlegungen lässt sich seine Arbeit zu nichtstaatlichen AkteurInnen im Cyberspace dennoch in den dazugehörigen Forschungsstrang einordnen.

14 Auf besagte Arbeiten wird im Zuge der Entwicklung des demokratischen Cyberproxy-Ansatzes im weiteren Verlauf noch genauer eingegangen.

1.3 Vergleich konventioneller und Cyberproxy-Funktionslogiken

Beim Vergleich von traditioneller Forschung mit der Cyberproxy-Forschung lassen sich folgende Unterschiede feststellen:

Die Überbrückung geografischer Distanzen ›at light speed‹
Für Proxy-Aktionen im Cyberraum ist es nicht notwendig, einen (offensiven) Proxy zu verwenden, der im Gebiet des Ziellandes stationiert ist.[15] Im Gegenteil: Immer mehr empirische Arbeiten zeigen, dass (hauptsächlich) autokratische Staaten nationale HackerInnen anheuern, anstatt die Mission an ausländische AkteurInnen auszulagern, über die sie keinerlei Kontrolle haben (für Iran: Anderson und Sadjadpour 2018; Russland: Carr 2011; Connell und Vogler 2017; China: Raud 2015).[16] Zudem kann die Versorgung der Proxy-AkteurInnen mit technischer Unterstützung erfordern, dass sie sich auf dem Territorium des Auftraggebers befinden, da nur hier die volle Kontrolle über die IT-Infrastruktur gegeben ist (Borghard und Lonergan 2016, S. 407). Außerdem ist es aus operativer Sicht für die Durchführung der meisten Cyberangriffe schlicht nicht notwendig, dass sich ein Proxy-Akteur im Land des anvisierten Ziels befindet (Brenner 2007).

Bezüglich des Spektrums staatlicher Verantwortlichkeit stellt die bloße Duldung der Tätigkeit von Proxys vom eigenen Staatsterritorium aus somit die niedrigschwelligste Staat-Proxy-Beziehung im Cyberspace dar, wie es vor allem im Hinblick auf Ransomware-Operationen russischer Cyberkrimineller seit 2021 verstärkt diskutiert wird (vgl. Hunnicutt 2021). Die im Falle traditioneller Proxys aktivere Unterstützung seitens des staatlichen Auftraggebers stellt somit einen weiteren Unterschied zur wissenschaftlichen Betrachtung von Cyberproxys dar, die von ihrem Staat auch lediglich geduldet werden können.

Aus dieser umgekehrten Stationierungslogik ergibt sich zudem, dass Cyberproxys im Gegensatz zu analogen Proxys zumeist in keinem Konflikt mit dem anvisierten Akteur stehen, also erst durch die Beauftragung des Staates zu einer Konfliktpartei werden. Eine Ausnahme hiervon sind vor allem patriotische HackerInnen und Cybermilizen.

AkteurInnen mit breitem Motivationsspektrum
Im Gegensatz zu ihren analogen Pendants weisen Cyberproxys ein noch vielfältigeres Spektrum an potenziellen Motiven für die eigene Rollenübernahme auf: Das ›MICE‹-Akronym (Money, Ideology, Coercion, Ego; Eoyang 1994), das zur Beschreibung der Motivationen konventioneller Spione verwendet wird, kann auch bei ihnen Anwendung finden. In der Literatur wird besonders von einigen ›Hired-Gun‹-Gruppierungen ausgegangen, etwa dem Russian Business Network (RBN), die bei entsprechender Bezahlung für nahezu jeden Auftraggeber arbeiten (Money) (vgl. Klimburg 2011, S. 49–50). Daneben existiert jedoch auch eine große Bandbreite an staatlich geförderten HackerInnen, die aus ideologischer Überzeugung oder Interessenskompatibilität an ihre Mission glauben (Ideology) (vgl. Staniland 2015).

---

15 »*Electrons are cheaper, faster, safer, and more easily deniable than human spies*« (Nye 2018).

16 Die bekannteste Ausnahme von dieser Praxis ist Nordkorea, welches vor allem in China, Indien aber auch Russland stationierte Proxys für Cyberattacken nutzt (Insikt Group 2017a).

Neben auf Freiwilligkeit basierenden Motiven nichtstaatlicher AkteurInnen können jedoch auch staatliche Zwangsmaßnahmen diese zur Proxy-Rollenübernahme bewegen. Bei einem kriminellen Aktivitätsprofil des Proxys kann diesem Strafe angedroht werden, falls er nicht auch Aufträge der jeweiligen Regierung übernimmt (Coercion). Schließlich kann das Ego der StellvertreterInnen ihr Engagement erklären: Für technisch ambitionierte HackerInnen offeriert die finanzielle und technische Unterstützung eines Staates ungeahnte Möglichkeiten bei der Durchführung von Cyberoperationen. Ein Handeln im Rahmen einer geheimen Staatsoperation kann zudem das Geltungsbedürfnis solcher AkteurInnen in besonderem Maße stärken. Dasselbe gilt auch für IT-Firmen, die in demokratischen Staaten durch zunehmend sophistizierte Attributionsberichte nicht nur ihre Gewinnmarge, sondern auch ihre Reputation im Allgemeinen stärken können. Zudem dürfte entsprechend des eigenen Selbstverständnisses als liberal-demokratisches Unternehmen auch eher solchen Regierungen durch die eigenen Aktivitäten gedient werden wollen.[17]

Verschleierung durch ›Plausible Deniability‹ (›plausible Abstreitbarkeit‹)

Der wichtigste (aber nicht ausschließliche) Vorteil, den ein Cyberproxy einem Staat bieten kann, ist die Schaffung der bereits erwähnten ›Plausible Deniability‹, wodurch letztlich die eigene Verantwortlichkeit verschleiert werden soll.[18] Dies gilt insbesondere für autokratische Staaten, die versuchen, ihre schadhaften Cyberaktivitäten durch die Anweisung und/oder Unterstützung eines dritten Akteurs zu verdecken. Im Gegensatz zu demokratischen Staaten haben Autokratien aufgrund ihrer illegitimen Cyberoperationen sowie der strukturellen Dominanz demokratischer Wert- und Normvorstellungen auf der Ebene der internationalen Beziehungen mehr Angst vor internationalen Rückschlägen als vor ihrer heimischen Bevölkerung.[19] Die Aufgabe des

---

17 Gestützt werden diese Annahmen auch durch den Artikel von Romanosky und Boudreaux aus 2021: Darin führten diese ExpertInneninterviews durch, um die unterschiedlichen Motivlagen privater und staatlicher AkteurInnen für öffentliche Cyberattributionen zu beleuchten. Die Befragten verwiesen für IT-Firmen vor allem auf deren Reputationsgewinne, aber auch deren Ansinnen, die breite Öffentlichkeit für Bedrohungen im Cyberspace zu sensibilisieren und somit die Debatte informierter zu gestalten.

18 Diese wird jedoch seitens Andrew Mumford auch für den Einsatz analoger Proxies als *ein* zentrales Motiv staatlicher Prinzipale in seinem Buch aus 2013 herausgestellt. Unter ›Verschleierung‹ wird im Rahmen der Arbeit eine gezielte Herstellung oder Manipulation bestehender Informations(a)symmetrien verstanden. Damit müssen nicht notwendigerweise eine völlige Geheimhaltung der eigenen Handlung bzw. Verantwortlichkeit hierfür einhergehen.

19 So zeigt das Beispiel Stuxnet, dass demokratische Staaten wie die USA und Israel aufgrund ihres schadhaften Cyberengagements gegen ›Schurkenstaaten‹ wie den Iran bislang keine internationalen Sanktionen oder Konsequenzen fürchten mussten. Auch wenn unilateral nahezu sämtliche demokratische StaatsführerInnen derlei Angriffe auf die kritische Infrastruktur eines anderen Landes generell verurteilt haben, so hat die demokratische Allianzkonstellation eine öffentliche Verurteilung der Cyberaktionen des Verbündeten (der zudem auf allen Ebenen überlegen/asymmetrisch mit Machtressourcen ausgestattet ist) bislang verhindert. Hinzu kommt, dass es neben den unilateralen Verurteilungen bislang noch zu keiner multilateralen, verbindlichen Erklärung über das Verbot von Cyberangriffen auf kritische Infrastrukturen gekommen ist, die über die UNGGE Berichte 2013/2015 hinaus geht.

legitimen Gewaltmonopols nach Max Weber ist, wie Maurer 2018a betont, für demokratische Regierungen weitaus kritischer als für ihre autokratischen Pendants, wenn auch ›nur‹ im Cyberspace.[20] Einen offensiven Cyberproxy zu verwenden, kann Autokratien somit vor bi- oder multilateralen Sanktionen schützen. Die selektive Strafverfolgung staatlicher HackerInnen wird dabei oftmals in Kauf genommen.

1.4 Staatliche Cyberproxy-Nutzung als rein offensives Metier?

Der Literaturüberblick und der Vergleich zeigen, dass sich die Proxy-Forschung bislang überwiegend auf die offensive Rolle nichtstaatlicher AkteurInnen fokussierte. Während in konventionellen Konflikten in erster Linie lokale Proxys unterstützt wurden und der staatliche Sponsor in den meisten Fällen eigentlich keine direkte Konfliktpartei ist, werden Proxys im Cyberspace vor allem genutzt, um andere Staaten mit oder ohne darunter liegendem konventionellen Konflikt zu schwächen oder zielunspezifische Vorteile durch den Angriff zu generieren (Cyberspionage). Das Motiv der Plausible Deniability scheint dabei für den Cyberspace eine noch größere Relevanz zu entfalten, begünstigt hier vor allem durch das noch zu behandelnde Attributionsproblem.

Der grundlegenden Proxy-Logik, im Sinne einer angestrebten Kostenvermeidung durch einen zwischengeschalteten Stellvertreter, folgen der Argumentation der Arbeit nach jedoch nicht nur autokratische Staaten. So haben Demokratien gerade aufgrund ihres Status als prominente Ziele autokratischer Cyberangriffe ein Interesse daran, die mit der Beantwortung dieser Vorfälle verbundenen Kosten durch den Einsatz defensiver Proxys regelmäßig zu vermeiden. Beide Cyberproxynutzungen interagieren somit und treffen als regimetypenspezifische Außenpolitiken auf außenpolitischer Ebene aufeinander. Im weiteren Verlauf der Arbeit wird auf demokratischer Seite insbesondere das Delegieren oder Anstoßen privat geführter Attributionsbemühungen seitens IT-Firmen als eine solch defensive Proxytätigkeit betrachtet. Hierfür wird auch geklärt werden, warum gerade dieser Aktivität besondere politische Bedeutung im Hinblick auf Kostenvermeidung demokratischer Regierungen zugesprochen wird. Im Sinne des liberalen Erklärungsansatzes wird somit aufgezeigt, welchen Nutzen diese defensiven Cyberproxys

---

20 Die nationalen und internationalen Gesetze der meisten demokratischen Staaten verbieten den Einsatz nichtstaatlicher Akteure in der Endphase der Verwaltung offensiver Cyberoperationen. Beispiele hierfür sind das US-Computerbetrugs- und Missbrauchsgesetz oder in Deutschland der sog. Hackerparagraph aus dem Jahr 2007 (§202 c, Strafgesetzbuch der Bundesrepublik Deutschland). Dagegen sind die meisten autokratischen Staaten wie Russland oder China früheren multilateralen Abkommen zur Regulierung von Cyberhacking-Bemühungen vom eigenen Territorium aus nicht beigetreten, wie der Budapester Cybercrime-Konvention aus 2001, einer Initiative des Europarates Grant 2012, S. 16.
Robert Gorwa und Max Smeets stellten folgende These auf: »*Based on the Plausible Deniability argument, we should expect democracies, as states with high levels of public accountability and greater attentiveness to reputational costs than authoritarian regimes, to primarily rely on these types of actors* [cyberproxies; Anm. d. Autorin]« 2019, S. 19. Somit handelt es sich hier um ein republikanisches Gegenargument zur These der beiden Autoren.

demokratischen Regierungen im zunehmend asymmetrisch geführten (Cyber-)konfliktaustrag gegenüber Autokratien bieten. Zudem wird begründet, warum der Begriff ›Proxy‹ im Attributionskontext gerechtfertigt erscheint und warum diese Art von StellvertreterInnen als kritischer und somit untersuchungswürdiger als demokratische Software-Unternehmen bewertet wird, die ihre Technologie nicht nur an autokratische Regierungen verkaufen.[21] Hierfür gilt es jedoch, zunächst das Attributionsproblem als technischen und politischen Untersuchungsgegenstand zu thematisieren.

1.5 Bisheriger Forschungsstand zum Attributionsproblem im Cyberspace

Cyberoperationen verdeutlichen die Besonderheit der einzigen von Menschen selbst erschaffenen »Fifth Domain« (Healey und Wilson 2012, S. 59). Die Grundkonzeption des Cyberspace, jedoch auch der fortschreitende technologische Fortschritt, erweitern das Angriffsspektrum potenzieller Cyberangreifer stetig und erlauben es ihnen, Angriffe weitgehend unerkannt und oftmals auch unentdeckt durchführen zu können. Wichtig ist, dass Attribution ›Detection‹ voraussetzt: Wenn der Angriff gar nicht erst entdeckt wird, weil die AngreiferInnen so subtil und technisch ausgefeilt agierten, kommt das sog. Attributionsproblem nicht zum Tragen, da die Frage nach dem Täter ohne erkennbare Tat gar nicht erst gestellt wird (Baram und Sommer 2019). Somit repräsentieren technische Methoden des Unerkanntbleibens die erste Hürde eines möglichen Attributionsprozesses. Prinzipiell können Methoden der ›*Internal Detection*‹ hierbei Abhilfe schaffen. Dabei handelt es sich etwa um ›Pattern-Matching‹ oder ›Signature-based Detection‹, wodurch als schadhaft einzustufende Netzwerkaktivitäten früher und besser erkannt werden können (Buchanan 2017, S. 56).

Sogenannte ›False-Flag‹-Attacken werden gemeinhin als eine der hauptsächlichen Herausforderungen der Attribution auf technischer, nachgelagert jedoch auch politischer Ebene angeführt. Hierbei verwenden AngreiferInnen technische Tools, die üblicherweise anderen AkteurInnen zugesprochen werden, um so eine falsche Fährte zu legen (Bartholomew und Guerrero-Saade 2016). Technische Methoden wie die Verwendung von Proxy-Servern zum Umleiten des mit dem Angriff verbundenen Datentransfers über Transitländer (Green 2016, S. 114–115) sowie die Instrumentalisierung fremder

21 Ein Unterschied existiert dennoch auch hier zwischen Demokratien und Autokratien: Während der Erwerb und die Nutzung kommerzieller Spionagesoftware von Firmen wie Gamma International oder der NSO-Group seitens demokratischer Staaten lange Zeit weniger kritisch diskutiert wurden, widmet sich etwa das Citizen Lab aus Toronto explizit in seinen Analysen autokratischer Spionagetätigkeit mithilfe solcher Software, da sich diese häufig gegen Dissidenten im In- und Ausland richten. Eine solche Nutzung ihrer Produkte schließen die internen Richtlinien besagter Firmen eigentlich aus und weisen jedwede Verantwortung für potenziellen Missbrauch von sich (Muth 2019). Die angebliche Nutzung der Pegasus-Spyware der NSO-Group seitens der spanischen Regierung gegen einen katalanischen Oppositionellen, aufgedeckt im Juli 2020, war jedoch ein erstes Indiz für das Aufbrechen dieser Regimetypenunterscheidung, welche durch die weiteren Enthüllungen im Sommer 2021 zur Pegasus-Nutzung demokratischer Akteure, darunter auch das deutsche BKA, weitere Nahrung erhielt (Flade und Mascolo 2021).

Computer zum Aufbau eines Botnetzes sind nur zwei weitere Beispiele potenzieller Verschleierungstaktiken (Knake 2010, S. 10).

Trotz aller existierender Vorteile für AngreiferInnen gibt es jedoch auch Grund zur Hoffnung aufseiten der IT-AnalystInnen: Die technischen Möglichkeiten zur Attribution wurden in den vergangenen Jahren erweitert, was nicht zuletzt auch der teilweise stattfindenden Kooperation verschiedener IT-Firmen zu verdanken ist.[22] Technische Indikatoren müssen jedoch zumeist mit geheimdienstlichen oder allgemeinen, politischen Argumenten und Evidenzen verknüpft werden, um Aussagen über die akteursbezogene Identität der AngreiferInnen tätigen zu können. Gerade das Ausmaß technischer Sophistiziertheit in Verbindung mit der funktionalen Ausrichtung der Attacke kann erste Erkenntnisse über den Angreifertyp liefern. Somit können oftmals weniger anspruchsvolle, weil opportunistischer agierende AkteurInnen, etwa Cyberkriminelle, aus dem Kreis der Verdächtigen ausgeschlossen werden. Ist für einen Angriff eine rein finanzielle Motivation auszuschließen, weist der Vorfall jedoch ein hohes Maß an technischer Komplexität auf,[23] wird meist eine staatliche Beteiligung unterstellt, insbesondere seit dem Bekanntwerden von Stuxnet (Guitton und Korzak 2013). Somit wurden rein technische Indikatoren in den politischen Gesamtkontext gestellt bzw. Erkenntnisse über Täter-Mittel-Zusammenhänge auf diesen übertragen und miteinander verknüpft. Weitere Indikatoren, die auf technischer Ebene oftmals mit generellen Evidenzen über die vermuteten TäterInnen verbunden werden, sind »*specific email addresses, certain patterns, specific name files, MD5 hashes, time stamps, custom functions and encryption algorithms*« (FireEye 2014, S. 29) sowie »*timestamps*«, »*strings*«, »*debug paths*«, »*metadata*« oder auch »*passwords*« (Bartholomew und Guerrero-Saade 2016, S. 1–2). Der Mehrwert dieser kontextbasierten Methode wird seitens Forschung (Rid und Buchanan 2015) und Politik (ODNI 2018) propagiert, um einen Ausweg aus der vermeintlich unüberwindbaren Hürde der »*True Attribution*«, also der konkreten Benennung von Akteurstypus und Herkunftsland, zu liefern (Lee 2016).

Darüber hinaus werden jedoch zunehmend die politischen Unwägbarkeiten von Attribution und deren öffentlicher Vermittlung seitens staatlicher, aber auch privater AkteurInnen in den Mittelpunkt öffentlicher Debatten gerückt (Lindsay 2015; Lohmann 2018; Poznansky und Perkoski 2018; Schulzke 2018; Romanosky und Boudreaux 2021). Die bereits beschriebenen technischen, damit verbunden jedoch auch strategischen Unterschiede verschiedener Attributionsarten standen dabei genauso im Mittelpunkt wie die unterschiedlichen Attributionslogiken vor, während und nach einer Attacke (Clark und Landau 2010). Andere BeobachterInnen stellten zunehmend auch die (geo-)politischen Abwägungen während dieser verschiedenen Attributionsstufen in den Mittelpunkt der Debatte, verbunden mit der Frage nach den Interessenlagen der jeweiligen Regierungen (Lin 2016). Aus sozialkonstruktivistischer Sicht wurde dagegen bereits die

22 Ein Beispiel hierfür ist der gemeinsame Bericht verschiedener IT-Firmen mit dem Titel »*Operation Blockbuster*« aus 2016, welcher sich im Zuge des Sony-Hacks mit der nordkoreanischen APT Lazarus beschäftigte (Novetta 2016).

23 Technische Indikatoren hierfür wären etwa die Verwendung von Zero-Day-Exploits oder gestohlener Software-Zertifikate (Saalbach 2019, S. 288).

soziale Konstruktion vermittelter Zusammenhänge zwischen dem Attributionsproblem und staatlichen Deterrence-Strategien thematisiert (Lupovici 2016).[24]

In der Forschung wurde in den letzten Jahren verstärkt die Frage thematisiert, welche Faktoren die jeweiligen Regierungen im Falle einer Cyberoperation auf nationale Zielsysteme zu einer *bewussten* Offenlegung und darüber hinaus zu einer Attribution bewegen können (Poznansky und Perkoski 2018; Baram und Sommer 2019; Canfil 2020). Den bislang umfassendsten Versuch einer Konzeptualisierung staatlicher Attributionsstrategien unternahmen Florian Egloff und Max Smeets 2021: In ihrem Artikel entwickelten sie ein ›Framework‹ für öffentliche Attributionsprozesse, das den Entscheidungsprozess politischer EntscheidungsträgerInnen anhand unterschiedlicher Kategorien abbilden soll (*»Geopolitics«, »Intelligence«, »Incident Severity«, »Handling und Follow-on-Actions«)*. Die hierbei erfassten operationsspezifischen, opfer- und angreiferspezifischen sowie kontextspezifischen (Timing und Beziehung zum attribuierten Akteur) Kriterien verdeutlichen die auch im Rahmen dieser Arbeit betonte Multidimensionalität öffentlicher Attributionsprozesse. Diese lassen sich eben nicht nur auf technische Indikatoren und Beweisführungen reduzieren, sondern werden immer stärker zum Gegenstand politischer Abwägungsentscheidungen auf nationaler und internationaler Ebene.

Für weitere Arbeiten spielten zudem demokratietheoretische Implikationen der Cyberattribution bereits eine Rolle. Dabei wurden speziell unzureichende Transparenzstandards der Regierungen im jeweiligen Prozess sowie deren Einfluss auf die Bedrohungsperzeptionen der Bevölkerungen problematisiert (Schulzke 2018). Aber auch die Rolle der Wissenschaft für einen wirksameren, öffentlichen Attributionsprozess wurde in den Mittelpunkt der Debatte gerückt, besonders im Hinblick auf angezweifelte Verantwortungszuweisungen (Egloff 2020a). Bis auf die beiden letztgenannten Quellen konzentrierten sich die bisherigen Arbeiten somit mehrheitlich auf die Rolle politischer Eliten im Rahmen von Cyberattributionsprozessen. Die potenziell steigende Bedeutung privatwirtschaftlicher AkteurInnen zur Kommunikation von Verantwortungszuweisungen auch gegenüber fremden Staaten wurde insbesondere durch die Arbeiten von Kristen Eichensehr aus den Jahren 2017, 2019 und 2020 stärker präsent. Daran anknüpfend untersuchten Sasha Romanosky und Benjamin Boudreaux 2019 die zunehmende Verflechtung zwischen politischen und privaten AkteurInnen bei der öffentlichen Aufarbeitung von Cyberoperationen, gestützt durch ExpertInnen-Interviews mit beiden Stakeholdergruppen.

1.6 Forschungsdesign

Im Rahmen eines regimetypenbasierten Erklärungsmodells wird in der Arbeit untersucht, welche Rolle und Funktionen nichtstaatliche AkteurInnen in den Cyberstrategien nationaler Staaten übernehmen können. Hierfür wird ein liberaler Erklärungsansatz

24 Dabei ging es konkret um die soziale Vermittlung von Bedeutungszusammenhängen der Konzepte ›Gewalt‹ und ›Anonymität‹ und welchen Einfluss diese sozialen Konstruktionen auf den Erfolg oder das Scheitern von ›cyber-deterrence‹ nehmen.

angeboten. Für Autokratien bedeutet dies die Proxy-Funktion offensiver Cyberoperationen, für Demokratien die Proxy-Funktion defensiver Attributionsbemühungen. Entsprechend der jeweils unterschiedlichen Regime-Logiken autokratischer und demokratischer Staaten beim Einsatz von Cyberproxys werden die Kosten, die von den als Cyberproxys auftretenden AkteurInnen anstelle des Staates getragen werden, unterschiedlich konzeptualisiert. Dies hat wiederum Einfluss auf die Frage, wer jeweils als staatlicher Proxy im Cyberspace zu gelten hat und wer nicht. ›Cyberproxys‹ werden definiert als *offiziell nichtstaatliche AkteurInnen, die für eine (oder mehrere) Regierung(en) eine Handlung im oder den Cyberspace betreffend ausführen, die ansonsten die Regierung selbst hätte tätigen müssen, was für Letztere mit hohen, regimetpyenabhängigen Kosten verbunden sein kann.* Anlehnend an Borghard und Lonergan (2016) und in Kontrast zu Maurers Definition werden somit auf autokratischer Seite lediglich vorbereitende Dienstleistungen im Hinblick auf eine solche Handlung *nicht* erfasst, weil hierbei letztlich die jeweilige Regierung final operativ tätig wäre. Ein Beispiel hierfür wären Software-Firmen, die Regierungen Spionagesoftware liefern, diesen jedoch keine Plausible Deniability bieten können, da die Ausführung der Cyberoperation letztendlich bei den staatlichen Einheiten verbleibt. Zudem verkaufen die erwähnten IT-Firmen öffentlichen Erkenntnissen nach ihre Produkte sowohl an Demokratien als auch an Autokratien. Regimetypenabhängige Faktoren scheinen hier somit weniger relevant zu sein.

Ähnlich wie bei Borghard und Lonergan wird in vorliegender Konzeptualisierung die unterschiedliche Motivlage nichtstaatlicher AkteurInnen betont, sich in die Rolle eines autokratischen Proxys zu begeben. Im Gegensatz dazu steht die einseitigere Konzeptualisierung der nach finanziellem Profit strebenden ›Cyber-Mercenaries‹.

Im Anschluss an das erste Kapitel wird der ›neue Liberalismus‹ nach Andrew Moravcsik als gewählter Theorierahmen diskutiert. Besonderer Fokus liegt dabei auf den gesellschaftlichen Interessen im Sinne der dreigliedrigen Ausdifferenzierung sowie den Interdependenzen als der von Moravcsik als zentral erachteten Präferenzkonstellation auf internationaler Ebene. Es sollen die Fragen beantwortet werden, inwiefern liberale Erklärungsansätze bisher in der Lage waren, konfliktive vs. kooperative Außenpolitiken demokratischer und autokratischer Staaten auf Grundlage welcher Prämissen zu erklären, wie sich der Ansatz des ›neuen Liberalismus‹ von den beiden Theoriesträngen des Institutionalismus und Realismus abgrenzt und warum er für das Erkenntnisinteresse der Arbeit als am sinnvollsten erachtet wird. Nachfolgend wird aufgezeigt, inwiefern die vorliegende Arbeit das Eigeninteresse politischer Führer noch stärker in den Mittelpunkt der Analyse stellt als Moravcsik und inwiefern hierdurch eine Manipulation von asymmetrischen Interdependenzverhältnissen nach innen und außen möglich wird. Dabei sollen folgende Fragen adressiert werden: Welche liberalen Hypothesen erscheinen auch für politische Handlungen im Cyberspace plausibel? Welche notwendigen Anpassungen müssen auf theoretischer Ebene vorgenommen werden, um dem Cyberspace als Konfliktaustragungsraum gerecht zu werden und außenpolitisches Verhalten hierin aus liberaler Perspektive heraus plausibilisieren zu können?

Nachfolgend werden die unterschiedlichen Chancen zur Durchsetzung eigener Interessen bzw. die strategischen Handlungsspielräume autokratischer und demokratischer Regierungen im bzw. mithilfe des Cyberspace gegenüber ihrer domestischen und internationalen Umwelt behandelt. Auf Grundlage dieser theoretischen Vorar-

beiten wird im dritten Kapitel das liberale, regimetypenabhängige Erklärungsmodell staatlicher Cyberproxynutzungsmuster konzeptualisiert. Dabei wird erläutert, welche Rolle unterschiedliche Cyberproxys bei der Manipulation antizipierter oder bereits bestehender asymmetrischer Interdependenzverhältnisse aus autokratischer und demokratischer Perspektive spielen können. Die zentrale unabhängige Variable des Erklärungsmodells stellen die jeweiligen domestischen Präferenzkonstellationen im Sinne Moravcsiks dar, da diese Ausdruck der Interessensdurchsetzungschancen verschiedener AkteurInnen auf republikanischer Ebene sind und aufzeigen, welche ideellen und wirtschaftlichen Präferenzen des Staates dies auf außenpolitischer Ebene zur Folge hat. Es wird zudem begründet, warum die jeweilige Umwelt des im Cyberspace agierenden Staates als konditionierende Variable sowie das allgemeine Konfliktniveau von Cyberkonflikten als intervenierende Variable bedeutsam sind. Die abhängige Variable der staatlichen Cyberproxy-Strategie wird nochmals unterteilt in Funktion und Art der Proxys, d.h., welche inhaltlichen Aufgaben sie für den staatlichen Auftraggeber übernommen haben und durch welche Akteurscharakteristika sie sich beschreiben lassen. Letztlich werden über das Wirken dieser einzelnen Bestandteile Hypothesen formuliert, die es im Rahmen der empirischen Analyse zu überprüfen gilt.

Als Hauptinstrumentarium hierfür wird ein Mixed-Methods-Ansatz verwendet: Auf Grundlage eines umfassenden Cyberkonfliktdatensatzes (HD-CY.CON) werden zunächst die übergeordneten Trends getestet: Nutzen tatsächlich in erster Linie autokratische Staaten offensive Cyberproxys gegen demokratische Staaten und sind es primär demokratische Länder, in denen IT-Firmen den Attributionsprozess übernehmen? Zudem soll geprüft werden, ob sich die bislang etablierte Vorstellung von staatlicher Zurückhaltung im Cyberspace auch auf Grundlage des HD-CY.CON bekräftigen lässt. Diese wurde bislang über rationale Kosten-Nutzen-Erwägungen der AkteurInnen erklärt, wobei die Effektivität von Cyberoperationen im Vergleich zu traditionellen Konfliktaustragungsmitteln angezweifelt wurde (Gartzke 2013; Valeriano et al. 2018; Borghard und Lonergan 2019). Eine zweite, sozialkonstruktivistisch geprägte Perspektive würde dagegen stärker die einhegende Wirkung bereits etablierter oder emergierender Normen im Cyberraum als Wirkfaktor herausstellen, gerade im Hinblick auf das bisherige Ausbleiben von Cyberangriffen mit letalen Folgen (Finnemore und Hollis 2016). Ein dritter Erklärungsansatz macht dagegen die Furcht vor ungewollten, analogen Eskalationsdynamiken primär für die bisherige Zurückhaltung von Staaten im Cyberspace verantwortlich (Valeriano und Maness 2014; Valeriano und Jensen 2019). Zuletzt wertet die neorealistische Perspektive die staatliche Zurückhaltung im Cyberspace als bloßes Nebenprodukt der globalen Machtverteilung nach dem Ende des Kalten Krieges (Healey und Jervis 2020). In vorliegender Arbeit wird stattdessen argumentiert, dass eine bislang dominante Zurückhaltung autokratischer sowie demokratischer Staaten im Cyberspace in erster Linie als interdependentes Produkt der jeweiligen Proxy-Strategien angesehen werden kann, deren Analyse das hauptsächliche Erkenntnisinteresse der Arbeit darstellt.

Wurde die Fallauswahl getroffen, erfolgt die empirische Analyse im Rahmen eines strukturiert-fokussierten Vergleiches nach George und Bennett (2005). Die hierfür abgeleiteten Vergleichsfragen dienen dabei in allen Fällen als implizit strukturierende Elemente der späteren Analyse. Unterstützt werden sollen die vier Fallstudien (auf auto-

kratischer Seite: Russland und China; auf demokratischer Seite: USA und Israel) für den Zeitraum von 2000–2019 durch einzelne, halbstrukturierte ExpertInneninterviews, deren Erkenntnisse neben Informationen aus Primär- und Sekundärliteratur aus Wissenschaft, Politik und IT-Sektor in die empirische Analyse einfließen.

2. Der neue Liberalismus zur Erklärung staatlicher Außenpolitiken

Liberale Theorieansätze zeichneten sich in der Vergangenheit insbesondere durch einen fortschrittsgetriebenen Charakter aus. So wurden Demokratisierungsprozessen, wirtschaftlichem Handel sowie internationalen Organisationen grundlegend kooperations- und damit oftmals auch friedensfördernde Effekte nachgesagt (Keohane 1984; Owen 1994; Oneal und Russet 1997; Oneal et al. 2003). Dies spiegelte sich in der Ausdifferenzierung der liberalen Theorie im Sinne des Institutionalismus und des Transnationalismus wider, die heute zumeist jedoch nicht mehr als liberale Ansätze verstanden werden. Als zentrale liberale Theorie der internationalen Beziehungen kann ab den 1990er Jahren der sog. ›neue Liberalismus‹ nach Andrew Moravcsik gelten. Im Gegensatz zu Institutionalismus und Transnationalismus rückte dieser das Verhältnis zwischen dem nicht mehr als einheitlich begriffenen Staat und domestischen AkteurInnen und somit die substaatliche Ebene in den Fokus der Analyse von Außenpolitik, aber im Ergebnis auch internationaler Politik.[1] In vorliegender Arbeit wird Moravcsiks Ansatz aufgegriffen, im Hinblick auf das Konzept der ›Interdependenz‹ (notwendigerweise) jedoch mit Überlegungen der institutionalistischen Strömung verbunden.

Eine realistische Betrachtung staatlicher Cyberproxy-Strategien wäre schon aufgrund des realistischen Fokus auf Staaten und deren Macht- bzw. Sicherheitsstreben ungeeignet und könnte die Rolle nichtstaatlicher AkteurInnen im Rahmen staatlicher

---

1 Weitere Vertreter des Liberalismus wie Ernst-Otto Czempiel, Michael Doyle, Bruce Russett, Robert D. Putnam und Thomas Risse sahen ebenfalls soziale Strukturen und Interessen als zentral für die Erklärung außenpolitischen Verhaltens von Staaten an (Zacher und Matthew 1995, S. 118). Moravcsik überführte diesen Schwerpunkt jedoch erstmals in eine kohärente, sozialwissenschaftliche Theorie, welche durch ihre inhaltliche Dreiteilung die Analyse besagter Präferenzen im Sinne der Differenzierung zwischen *Polity, Politics* und *Policy* umfassender möglich machte. Zudem lieferte die Theorie durch die Integration von Elementen des Institutionalismus (Interdependenz) sowie des Zwei-Ebenen-Ansatzes (internationaler Handlungsspielraum nationaler Regierungen) direkte Anknüpfungspunkte zur Untersuchung der Wirkweise der zu erklärenden Außenpolitik auf internationaler Ebene. Diese Anleihen bei anderen Theorievertretern, sowie das gleichzeitige Beharren auf dem Alleinstellungsmerkmal als einziger, liberaler IB-Theorie (Moravcsik 1997, S. 516), kann jedoch gleichzeitig wissenschaftstheoretisch kritisiert werden.

Interessensdurchsetzung nicht erfassen. Der liberale Institutionalismus dagegen betont Möglichkeiten zur Überwindung der Anarchie durch Staaten, die nicht nur nach Macht und Sicherheit streben, nimmt deren Präferenzen jedoch als gegeben an und ist somit ebenfalls nicht in der Lage, die Entstehung staatlicher Cyberproxy-Strategien auf Grundlage der domestischen Präferenzbildung zu erklären. Zuletzt wird dem neuen Liberalismus nach Moravcsik auch gegenüber dem Sozialkonstruktivismus nach Wendt der Vorzug gegeben, da er ein stringenteres sozialwissenschaftliches Analysemodell des konkreten Einflusses spezifischer Interessen, die auch im Liberalismus auf Ideen und Werten basieren können, offeriert.

Warum und auf welche Weise dies für den Cyberspace im Allgemeinen und den Proxy-Gebrauch im Besonderen gerechtfertigt ist, wird im nachfolgenden Kapitel erläutert. Zunächst wird jedoch der neue Liberalismus vorgestellt.

2.1 Der neue Liberalismus als sozialwissenschaftlich-analytische Theorie

Andrew Moravcsik entwickelte seinen ›neuen Liberalismus‹ als direkte Antwort auf die Ende der 1990er Jahre vorherrschenden IB-Großtheorien des Realismus und Institutionalismus.[2] So sei der Liberalismus eine ernstzunehmende und aus empirischer Sicht ebenbürtige Alternative zu den genannten Konkurrenztheorien, analytisch jedoch gleichzeitig »*more fundamental*« (Moravcsik 1997, S. 513). Die vormals in erster Linie hinsichtlich ihrer teleologischen Komponente, dem immanenten Glauben an Kooperation und Frieden, geprägte Strömung des Liberalismus galt es hierfür jedoch aus Sicht Moravcsiks erst noch als eigenständige IB-Theorie zu etablieren. Die zentralen Analysekategorien seien dabei die Forderungen der sozialen AkteurInnen, die kausalen Mechanismen der Überführung der Forderungen in politische Entscheidungen sowie die daraus entstehende Präferenzkonstellation der Staaten auf internationaler Ebene (Moravcsik 1997, S. 524). In seinem Ursprungswerk von 1997 formulierte Moravcsik drei Grundannahmen, die die Basis seiner drei Liberalismus-Varianten bilden:

»The Primacy of Societal Actors«

Zentrale AkteurInnen im Liberalismus sind Individuen und soziale Gruppen. Diese seien (wie im Realismus und Institutionalismus) als generell rational und risikoavers zu charakterisieren und handeln im Rahmen von gegebenen Strukturbedingungen wie »*materi-*

2 Der ebenfalls von Moravcsik entwickelte liberale Intergouvernementalismus, welchen er anhand der regionalen Integration der EU ableitete und testete (Moravcsik 1993), ist nicht Gegenstand der vorliegenden Arbeit. Stattdessen werden im weiteren Verlauf Elemente des neoliberalen Institutionalismus in das Erklärungsmodell integriert, um die Auswirkungen der domestischen Präferenzbildung nach Moravcsik auf außenpolitischer Ebene und im Kontext der interdependenten Strukturmerkmale der Globalisierung und Digitalisierung umfassender analysieren zu können. Da der neoliberale Institutionalismus, wie auch der liberale Intergouvernementalismus, Staaten als die zentralen AkteurInnen auf internationaler Ebene ansieht, findet dadurch kein Bruch der Forschungslogik statt.

al scarcity, conflicting values, and variations in societal influence« (1997, S. 516).[3] Als grundlegende Strukturbedingung der AkteurInnen begreift Moravcsik dabei die Globalisierung, die positive oder negative Anreize zum Eintritt in den Bereich der »*world politics*« setzt (Moravcsik 2013, S. 3). Globalisierung determiniert gleichzeitig als Kontextfaktor die Anforderungen der sozialen AkteurInnen an die politischen EntscheidungsträgerInnen. Diese Anforderungen werden somit als endogene Ursachen für das jeweilig staatliche Interesse im Sinne der nachfolgend zentralen »*Preferences*« angesehen. Gleichzeitig resultieren diese dem Ansatz nach nicht automatisch in einer harmonischen Außenpolitik des jeweiligen Staates, sondern können in Kombination mit einer entsprechend gelagerten domestischen Präferenzkonstellation anderer Staaten ebenso zum Konflikt führen. Nämlich dann, wenn eine oder mehrere der drei Komponenten »*divergent fundamental beliefs, scarcity of material goods, and inequalities in political power*« präsent wären, aus denen sich die nachfolgend beschriebenen Variationen des liberalen Ansatzes ableiten lassen (Moravcsik 2003, S. 162–163).

»Representation and State Preferences«

Als zentrale AkteurInnen werden im Gegensatz zum Realismus somit nicht mehr nur die am Ende der politischen Entscheidungskette stehenden ›Staatsmänner‹ betrachtet, sondern sämtliche Individuen und Gruppierungen, die Einfluss auf den politischen Willensbildungsprozess haben.[4] Staatliche Institutionen seien somit immer nur ein ›*subset*‹ derjenigen domestischen AkteurInnen, deren Präferenzen sie in politische Handlungen transformieren (1997, S. 518).[5] Hinsichtlich der Akteurschaft von Regierungen unterscheidet Moravcsik zwischen nationaler und internationaler Ebene:

3 Moravcsik wendet dabei jedoch eine Form der ›bounded rationality‹ an, indem er erklärt, dass die gesellschaftlichen Präferenzen auf substaatlicher Ebene sehr wohl unterschiedlich und variant sein könnten, diejenigen, die sich letztlich jedoch auf politischer Ebene durchsetzen, vonseiten des Staates auch rational verfolgt werden würden (Moravcsik 1998, S. 21–23).

4 Im Institutionalismus werden ebenfalls in erster Linie Staaten als handelnde AkteurInnen betrachtet, zusätzlich jedoch auch internationale Organisationen sowie Regime, welche laut Keohane, Nye und Anderen, Staaten in ihrer Politik vor allem kooperationsfördernd beeinflussen können (Keohane und Nye 1987). Laut Moravcsik könnten auch subnationale, transnationale oder supranationale Institutionen die Rolle des Staates im Gefüge der Interessenvermittlung einnehmen, letztere stellen jedoch de facto nach wie vor die dominanten politischen Einheiten auf internationaler Ebene dar (Moravcsik 2013, S. 7).

5 Moravcsik betont dabei, dass »*preferences*« im liberalen Sinne unabhängig von zwischenstaatlichen, strategischen Interaktionen, wie etwa externen Bedrohungen oder positiven Anreizen gebildet würden und über Zeit relativ stabil seien. Er versäumt es hierbei jedoch, konkrete Beispiele zu nennen. Strategien und Taktiken seien dagegen eher als Policy-Optionen zu werten, welche aufgrund externer Einflüsse einem stärkeren Wandel unterliegen würden (2003, S. 164). Zudem wertet er Konzepte wie »*sovereignty*« und »*national defense*« nicht als Präferenzen, sondern als »*fundamental strategies*«, welche wiederum eigentlich vorgelagerten Präferenzen dienen sollen (2013, S. 4). Warum jedoch etwa der von ihm als Präferenz bezeichnete »*militant nationalismus*«, oder auch die »*fascist rule*« nicht ebenso als strategische Mittel zum Durchsetzen anderer Präferenzen angesehen werden könnten, bleibt aus Sicht der Autorin an dieser Stelle unklar (2013, S. 4). Zudem erscheint gerade für autokratische Staaten eine bestimmte auf Kontrolle, Zensur und Überwachung ausgerichtete Form der digitalen Souveränität ebenfalls eine Präferenz im Bereich der Internet Governance zu sein (Epifanova 2020).

> »Internationally, the liberal state is a purposive actor, but domestically it is a representative institution constantly subject to capture and recapture, construction and reconstruction, by coalitions of social interests« (Moravcsik 2013, S. 4).

Auf der internationalen Ebene handeln Staaten somit rational und orientieren sich an den auf domestischer Ebene vorherrschenden Interessen. Hinsichtlich der Durchsetzung dieser Präferenzen haben nationale AkteurInnen, sobald einmal die Ebene der internationalen Politik betreten wurde, jedoch laut Moravcsik keinen Einfluss mehr. Die strategische Handlungsautonomie der Regierungen ist hier im Sinne des Zwei-Ebenen-Spiels somit im Gegensatz zur domestischen Ebene erweitert, wo Regierungen bei Moravcsik stärker lediglich passive InteressenkonsumentInnen am Ende des Transmissionsriemens darstellen, als auf internationaler Ebene. Während Präferenzen aus realistischer Sicht naturgemäß konfliktiv und aus institutionalistischer Sicht als weitgehend konvergent anzusehen sind, ermöglicht der neue Liberalismus somit die Analyse domestischer Präferenzen über verschiedene Politikfelder hinweg, mit unterschiedlichen Interessengruppen als Ursprung (Moravcsik 1997, S. 520).

Die domestische Interessenaggregation durch den Staat fungiert somit als der sog. ›Transmission-Belt‹, durch den die domestischen Interessen auf die politische Ebene übertragen werden. Dessen Struktur sei dabei für die Analyse von Außenpolitik keinesfalls irrelevant, da der jeweilige Herrschaftszugang unterschiedlicher Interessengruppen variante Formen annehmen könne. Liberale Demokratien stehen dabei totalitären Diktaturen aufgrund der auf der einen Seite maximalen und auf der anderen Seite minimalen Inklusion und Repräsentation substaatlicher AkteurInnen konträr gegenüber (Moravcsik 2003, S. 163). Des Weiteren differenziert Moravcsik zwischen AkteurInnen außerhalb und innerhalb des staatlichen Systems, zentralisierter vs. dezentralisierter Interessenvermittlung, unterschiedlichen Rationalitätsniveaus der politischen Repräsentation, unterschiedlichen Sozialisierungen bezüglich risikobehafteten Verhaltens der politischen EntscheidungsträgerInnen und Institutionen sowie potenziellen Elementen direkter Repräsentation (Moravcsik 2013, S. 5).

»Interdependence and the International System«

Staaten werden in ihren Handlungen durch existierende und im Zuge der Globalisierung ansteigende Policy-Interdependenzen beeinflusst. Sie agieren somit nicht im luftleeren Raum, sondern verbinden Entscheidungen in einem Politikfeld notwendigerweise mit Überlegungen über deren Auswirkungen in anderen Sektoren, z.B. können Politikentscheidungen auf sicherheitspolitischer Ebene auch den Wirtschaftsbereich betreffen und umgekehrt (Moravcsik 1997, S. 520). Gleichzeitig ergeben sich für Staaten durch das Zusammenspiel mit den Interessen anderer Staaten Beschränkungen für die eigene Präferenzdurchsetzung. Die erwähnten Policy-Interdependenzen beschreibt Moravcsik dabei als das theoretische Verbindungsstück zwischen varianten staatlichen Präferenzen und letztlichem Handeln. Er definiert sie als

> »the set of costs and benefits for dominant social groups in foreign societies (the pattern of transnational externalities) that arise when dominant social groups in a given society seek to realize their own preferences internationally« (Moravcsik 2003, S. 165).

Wie der Institutionalismus sieht der neue Liberalismus in dieser interdependenten Präferenzkonstellation eine »*asymmetrical interdependence*«,[6] die politisches Verhalten entsprechend beschränken würde (Moravcsik 2003, S. 165).

Staatliche Interessen als Ausdruck domestischer Präferenzordnungen bilden somit das Herzstück des neuen Liberalismus. Über das finale Politikresultat Konflikt vs. Kooperation entscheidet dabei die jeweilige Präferenzkonstellation auf zwischenstaatlicher Ebene. Policy-Interdependenzen lassen sich dabei in die Kategorien ›zero-sum/deadlocked‹, ›harmonious‹ und ›mixed‹ einteilen. Im ersten Falle ist das Erreichen der Ziele der dominanten sozialen Gruppen in einem Land nur durch hohe Kosten in einem anderen Land möglich. Somit existieren in dieser Situation wenige Anreize für Kooperation und viele für Konflikt zwischen den Staaten. Im Gegensatz dazu beschreiben harmonische Policy-Interdependenzen Situationen, in denen sich die staatlichen Präferenzen in ihrem Erreichen nicht im Wege stehen und Kooperation somit wahrscheinlich ist. Dieser Fall ähnelt am ehesten der von den beiden Institutionalisten Keohane und Nye beschriebenen ›komplexen Interdependenz‹, die sie als idealtypischen Gegenentwurf zu einer konfliktiven internationalen Politiksphäre der realistischen Theorietradition zeichneten (Keohane und Nye 1987). Als wahrscheinlichster Realtypus kann jedoch der dritte Fall gelten: Hierbei treten Staaten in einen Verhandlungsprozess, in dem sie durch Anpassungen ihrer Erwartungen oder einer veränderten Informationslage eine für beide Seiten vorteilhafte Politikkoordination erreichen können (Moravcsik 2003, S. 166–167). Konflikt oder Kooperation ist hierbei somit nicht vordeterminiert, sondern kann durch das staatliche Management der Interdependenzsituation verhindert oder begünstigt werden.[7]

Entgegen geäußerter Kritiken (z.B. Rathbun 2010, S. 4) verbleibt der Liberalismus somit nicht auf einer der drei IB-Analyseebenen, sondern negiert deren Sinnhaftigkeit aus analytischer Sicht. Die enge Verquickung zwischen domestischen Interessen, deren Ausdruck in nationalen Politiken sowie deren Auswirkungen im Zusammenspiel mit den Präferenzen anderer Staaten im internationalen System machten diese Unterscheidung zunehmend obsolet. Somit sei gerade der Liberalismus als ›systemische‹ Theorie zu verstehen, die Präferenzen als zentrale Erklärungsfaktoren begreife, im Gegensatz zu den materiellen, machtpolitischen ›Capabilities‹ des (Neo-)Realismus oder der ›Information‹ bereitstellenden Institutionen des Institutionalismus (Moravcsik 2003, S. 165).

Ähnlich wie der Institutionalismus bescheinigt auch der neue Liberalismus der Ebene der internationalen Politik eine zunehmend steigende Verflechtung und Vernetzung und, damit einhergehend, auch ein immer heterogeneres Spektrum an domestischen AkteurInnen, vor allem im demokratischen Politikprozess. Außenpolitische Entscheidungen seien aus liberaler Sicht somit primär als das »*management of globalization*« (Moravcsik 2013, S. 14) zu verstehen. Daher eignet sich der Liberalismus auch besonders für eine Analyse außenpolitischer Entscheidungen in einem solch weithin vernetzten und

---

6 Oder auch »*relative intensity*« der Präferenzen (Moravcsik 2013, S. 6).

7 Für den Institutionalismus spielen internationale Institutionen und Organisationen hierbei eine entscheidende Rolle, da sie Regeln der Politikkoordination für die Zukunft festlegen, Anreize für betrügerisches Verhalten reduzieren und Fehlverhalten konsequent sanktionieren können (Keohane und Martin 1995, S. 42).

globalisierten Konfliktraum wie dem Cyberspace. Der Begriff der Globalisierung entstand bereits lange vor dem World Wide Web, das die Auswirkungen der Globalisierung jedoch im Sinne kaum noch geltender nationaler Grenzen im Cyberspace transformiert hat. Die Aufrechterhaltung traditioneller, staatlicher Souveränität im Cyberspace wird daher oftmals als illusorisch angesehen (Mueller 2020). Gleichzeitig zeigen differenzierte Zugänge zum Konzept der »Cyber-Souveränität« auf, dass gerade im Bereich der Infrastruktur, die nicht den Kernbereich staatlicher Souveränität betreffen, flexiblere Aushandlungsprozesse möglich wären (Rosenbach und Chong 2019). In jedem Falle erwachsen Anpassungserfordernisse für staatliche AkteurInnen: einerseits um nationale (oder Regime-)Interessen zu schützen, andererseits um die Vorteile der steigenden Vernetzung zu nutzen.

Die nachfolgenden Unterarten der liberalen Theorie sind als Komplementäre zueinander zu verstehen, die sich gegenseitig beeinflussen können. Ein möglichst umfassender Erklärungsansatz staatlicher Cyberproxy-Strategien muss das Analysepotenzial aller drei Varianten stets in Betracht ziehen, auch wenn nicht jede gleichermaßen erklärungskräftig für den jeweiligen Fall sein wird.

2.1.1 Normen und Werte als politische Leitlinien im ideellen Liberalismus

Soziale Präferenzen bezüglich kollektiver Güter wie »*national unity, legitimate political institutions, and socioeconomic regulation*« (Moravcsik 1997, S. 524) und deren Kompatibilität stehen bei der ersten Variante des Liberalismus nach Moravcsik im Mittelpunkt. Soziale Identitäten und Werte werden als Hauptbestimmungsfaktoren der späteren staatlichen Präferenzen angesehen, wobei »*social identities*« definiert werden als

> »the set of preferences shared by individuals concerning the proper scope and nature of public goods provision, which in turn specifies the nature of legitimate domestic order by stipulating which social actors belong to the polity and what is owed them.« (1997, S. 525).

Soziale Identitäten entscheiden somit über das Ausmaß und die Art der Bereitstellung öffentlicher Güter. Deren Herkunft sei entweder historisch oder durch bestimmte kollektive oder staatliche Handlungen bedingt, die von Moravcsik jedoch nicht konkretisiert werden (Moravcsik 2013, S. 7). Ob die Identitäten letztlich ideelle oder materielle Faktoren widerspiegeln würden, lässt der neue Liberalismus ebenfalls offen. Laut Moravcsik sind es drei Bestandteile der domestischen Ordnung, die durch diese sozialen Identitäten besonders geformt würden: »*geographical borders, political decision-making processes, and socioeconomic regulation*« (Moravcsik 1997, S. 525).[8] Ziel der nationalen Politiken müsse es stets sein, die Legitimität der drei Komponenten aus Sicht der relevanten sozialen AkteurInnen zu gewährleisten, da diese dem politischen System ihre Unterstützung nur in einem solchen Falle gewähren würden. Ob beispielsweise politische Institutionen als

8 In einem Beitrag von 2013 benennt er diese drei Aspekte etwas anders, hier spricht er von »*national identity, political ideology, and socioeconomic order*« (Moravcsik 2013, S. 7), gemeint ist hiermit jedoch wohl im Kern dasselbe.

legitim erachtet werden, hängt von deren Kompatibilität mit den beschriebenen sozialen Identitäten ab. Entsprechend der dritten Grundannahme des Liberalismus nach Moravcsik entscheidet wiederum die Kompatibilität dieser identitätsbasierten Staatspräferenzen über den Zustand der internationalen Beziehungen, d.h., ob diese eher konfliktiv oder harmonisch geprägt sind.[9] Durch beiderseitige Anpassungen in verschiedenen Politikfeldern könne jedoch auch im Falle zuvor nicht gänzlich zusammenpassender nationaler Einstellungen Kooperation ermöglicht werden (Stichwort Policy-Linkage; Lohmann 1997).

Ideelle Präferenzen setzen sich grundlegend aus drei Bestandteilen zusammen: Der erste Bestandteil sind die jeweiligen Vorstellungen der sozialen Gruppen von ihrer nationalen Identität. Diese beinhaltet soziokulturelle, historisch gewachsene sowie linguistische Aspekte der eigenen Nationenerzählung.[10] Aber auch die nationalen Grenzen im Sinne territorialer Souveränität sowie Fragen der Staatsbürgerschaft werden durch diese Form der Identität mitbestimmt und entsprechende Politiken auf internationaler Ebene somit in Richtung Kooperation oder Konfrontation geleitet (Moravcsik 1997, S. 525–526). Daran anknüpfend attestiert etwa die Forschung zum demokratischen Frieden demokratischen Gesellschaften immer wieder Tendenzen zu gewaltfreien Konfliktlösungsmechanismen sowie Kompromissbereitschaft, was sich durch Sozialisationsprozesse auch auf die jeweils Regierenden übertragen würde (Rousseau et al. 1996, S. 513).

Der zweite Hauptbestandteil ideeller Präferenzen betrifft die Verbundenheit bzw. das Pflichtgefühl (englisch ›Commitment‹) der sozialen AkteurInnen in Bezug auf die jeweiligen politischen Institutionen. Laut ideellem Liberalismus kann das in Staat A als legitim erachtete politische System die Realisierung der in Staat B als legitim erachteten öffentlichen Ordnung behindern, insbesondere, wenn die jeweiligen Vorstellungen hierüber konträr zueinander sind.[11] Diese Argumentation kann als Grundstein für das Theorem des demokratischen Friedens angesehen werden, da (liberale) demokratische Staaten grundlegende Vorstellungen über legitime politische Arrangements und Institutionengefüge prinzipiell gemeinsam haben sollten, um Frieden zu bewahren (Owen 1994). Der interne, demokratische Politikstil, der auf eine friedliche Konfliktbeilegung ausgerichtet ist, wird in diesem Falle somit gegenüber anderen Demokratien externalisiert.

---

9 Man könnte argumentieren, dass die ideelle Variante des neuen Liberalismus an die von Goldstein und Keohane 1993 vorgenommene Inkorporierung von Ideen als bedeutsamen Einflussfaktor auf staatliche Präferenzbildung anknüpft (Goldstein und Keohane 1993).

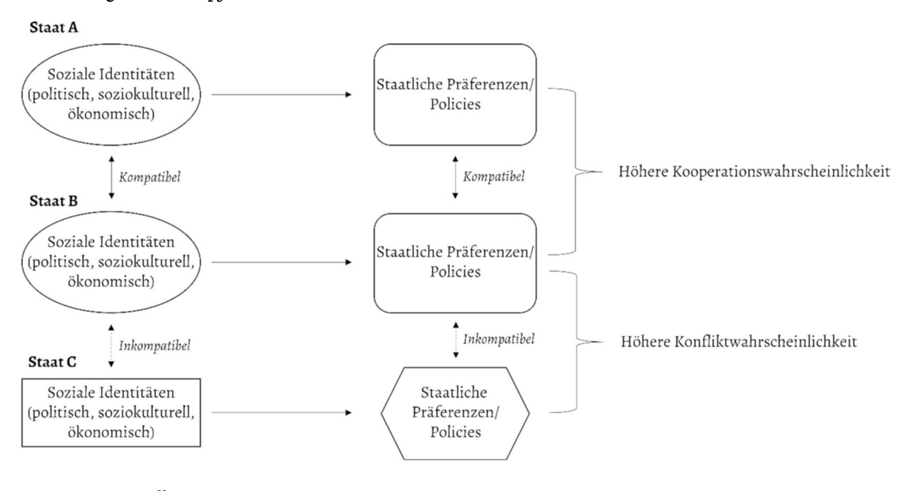
10 Unter Nationenerzählung wird in diesem Kontext das historisch geprägte Narrativ einer Nation über ihre Entstehung und Entwicklung im Laufe der Zeit verstanden, mit jedoch potenziell konkurrierenden Identitäts- und Bedeutungselementen, welche seitens unterschiedlicher Gruppierungen propagiert werden.

11 Wie bereits erwähnt, herrscht insbesondere bezüglich der Definition und Legitimität des Konzepts der nationalen Souveränität im Cyberspace bislang Uneinigkeit zwischen den Staaten (Giles 2012; Mueller 2017). Konkurrierende Ansätze hierüber sowie deren Wirkung auf die jeweilige Cyberproxy-Strategie können somit durch die Analyse der jeweilig ideellen Präferenzen analytisch eingefasst und für die empirische Analyse fruchtbar gemacht werden.

Drittens entscheidet laut Moravcsik die »*nature of legitimate socioeconomic regulation and redistribution*« (1997, S. 527) mit über das jeweilige außenpolitische Verhalten und durch Interaktionsmechanismen somit auch über die Konstellation der internationalen Beziehungen. Auch hier führen potenziell negative oder positive Externalitäten zum jeweiligen zwischenstaatlichen Verhaltensmuster. Im Vorfeld geteilte Werte könnten somit ein grundlegendes Erfordernis etwa für ein gemeinsames Vorgehen von Staaten in regulatorischen Bereichen wie Besteuerungen, Migration und auch der Außenpolitik darstellen. Potenzielle Autonomieverluste der nationalen Präferenzen durch notwendige Kompromisse auf der zwischenstaatlichen Ebene seien dabei jedoch ebenfalls vorstellbar und empirisch zu beobachten (Moravcsik 1997, S. 528).

Zusammenfassend sind laut ideellem Liberalismus insbesondere die sozialen Identitäten auf politischer, soziokultureller sowie ökonomischer Ebene eines Landes für die Interessensartikulation und Policy-Formulierung entscheidend. Inwiefern diese identitätsbasierten nationalen Politiken auf zwischenstaatliche Übereinstimmung treffen, entscheidet somit über Konflikt oder Kooperation. Regierungen müssen durch das Management der oftmals vorliegenden Policy-Interdependenzen dennoch versuchen, unter den Bedingungen konfliktiver Präferenzkonstellationen zu anderen Staaten die domestischen Präferenzen bestmöglich in außenpolitische Handlungen zu überführen.[12]

Abbildung 1: Kausalpfad des ideellen Liberalismus nach Moravcsik



(Eigene Darstellung)

12 Moravcsik erhebt einen Geltungsanspruch seines Ansatzes sowohl für liberale, als auch nicht-liberale Staaten (1997, S. 515). Was jedoch die zentralen Charakteristika einer Autokratie im Gegensatz zu einer Demokratie für die domestische Interessenvermittlung im Sinne des Transmissionsriemens bedeuten, wird im Rahmen der republikanischen Liberalismusvariante genauer erläutert werden.

2.1.2 Der Primat der Wirtschaft im ökonomischen Liberalismus

Der kommerzielle Liberalismus argumentiert aus einer stärker funktionalistischen Sicht auf die Strukturbedingungen des Marktes: Ändern sich die nationalen oder globalen Marktbedingungen, hat dies Auswirkungen auf nationale Regierungen. Diese sehen sich vonseiten der nationalen AkteurInnen zu protektionistischen Handlungen oder zu wirtschaftlichen Öffnungen gezwungen. Dabei betont Moravcsik, dass der Theorieansatz keinesfalls als deterministische Vorhersage der Dominanz kapitalistischer Wirtschaftsstrukturen und damit einhergehend von Frieden zu verstehen sei. Vielmehr ginge es dabei um die Beschreibung von Anreizsystemen, die sich aus Veränderungen der jeweiligen wirtschaftlichen Umwelten speisen und somit zu einer entsprechenden Anpassung nationaler Politiken führen, um entweder etwaige Kosten zu vermeiden oder nach potenziellen Gewinnen zu streben (Moravcsik 1997, S. 528).[13] Im Gegensatz zu (Neo-)Realismus, Institutionalismus und (Sozial-)Konstruktivismus, die Sicherheitsexternalitäten, informationelle und institutionelle Beschränkungen sowie identitätsbasierte Sozialisierungsprozesse für das Streben von Staaten nach relativen Gewinnen verantwortlich machen, argumentiert der kommerzielle Liberalismus mit dem Entstehen und Verlauf domestischer und globaler Verteilungskämpfe (Moravcsik 2013, S. 9).[14] So sei überall dort, wo ein hohes Maß an Wettbewerb sowie »*extensive intra-industry trade, or trade in intermediate goods, large foreign investments, and low asset specificity*« (Moravcsik 1997: 529) die heimische Wirtschaft prägen, freier und offener Handel auch wahrscheinlicher. Je anpassungsfähiger, konnektiver und ausgerichteter auf den Austausch mit grenzüberschreitenden Industrien die dominanten, domestischen WirtschaftsakteurInnen sind, desto größer ist der Druck auf die nationalen Regierungen, hierfür die entsprechenden Rahmenbedingungen zu schaffen. Widersprechen sich nationale Wirtschaftspolitiken in einer Weise, dass sie sich in ihrer jeweiligen Zielerfüllung potenziell behindern, ist eine konfrontative Interaktion zwischen den jeweiligen Staaten wahrscheinlicher.

Wirtschaftliche Interessenverfolgung führt auf internationaler Ebene somit auch zu gewaltsamen Konflikten. Laut kommerziellem Liberalismus ist dies vor allem der Fall, wenn Zwangsmaßnahmen zur Durchsetzung wirtschaftlicher Interessen auf domestischer oder internationaler Ebene angewandt werden. Monopolistische Wirtschaftsstrukturen spielten etwa im Rahmen der Kolonialisierung hierbei insofern eine wichtige Rolle, als die beteiligten AkteurInnen aufgrund des niedrigeren Grades an wirtschaftlicher Verflechtung im In- und Ausland im Falle der Anwendung von Gewalt auch weniger negative Konsequenzen zu befürchten hatten (Moravcsik 1997: 530).

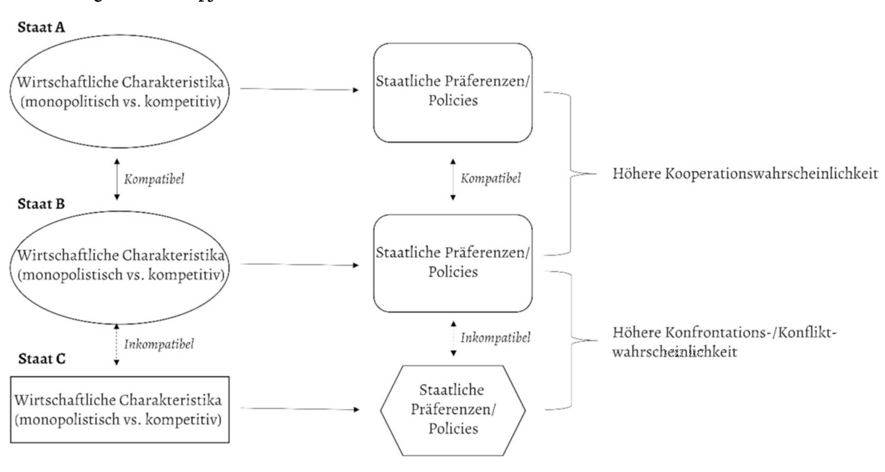
13 Die im ideellen Liberalismus zentralen sozialen Identitäten können einen Einfluss auf die ökonomischen Interessen eines Staates haben und umgekehrt. Somit lassen sich die ersten beiden Liberalismus-Stränge nicht völlig getrennt voneinander betrachten.

14 Zudem negiert der Liberalismus zwar keinesfalls die Bedeutung von Ideen im Allgemeinen, welche im Konstruktivismus eine zentrale Rolle in der Überwindung der rein systemischen Theorieansätze darstellen, stellt jedoch darüber hinaus auch deren konkreten Einfluss auf den politischen Entscheidungsprozess in den Vordergrund. Somit soll im Liberalismus geklärt werden, warum gerade diese und jene Ideen die politischen Entscheidungen maßgeblich mitgeprägt haben (van Apeldoorn und Graaff 2014, S. 32).

Entwicklungen hin zu mehr Diversifizierung, Spezialisierung und Arbeitsteilung auf dem globalen Weltmarkt führten jedoch zu einer immer größeren Kriegsaversion wirtschaftlicher AkteurInnen, da sie hierdurch längerfristig meist mehr zu verlieren als zu gewinnen hätten.[15]

Zusammengefasst entscheiden somit laut kommerziellem Liberalismus die Präferenzen der dominanten, domestischen Interessengruppierungen auf kommerzieller Ebene darüber, ob eine konfliktive oder kooperative Wirtschaftspolitik gegenüber anderen Staaten verfolgt werden kann. Je größer die Inkompatibilität zwischen den eigenen, kommerziellen Interessen sowie denen des anderen Staates, desto schwerer scheint auch das konfliktfreie Interdependenzmanagement der besagten Staaten zu werden. Eine Inkompatibilität kann dabei auch zwischen den ökonomischen Präferenzen eines Staates A und den eher ideellen Präferenzen eines Staates B existieren, etwa indem privatwirtschaftliche Interessen bestimmter Gruppierungen den allgemeinen Werte- und Güterverteilungsmodus eines anderen Landes bedrohen. Welche Präferenzen in Staat A oder B den Vorzug erhalten, ist auch von den politischen Institutionen abhängig, die Interessen zumeist unterschiedlich stark repräsentieren (Moravcsik 2013, S. 5–6).

Abbildung 2: Kausalpfad des kommerziellen Liberalismus nach Moravcsik



(Eigene Darstellung)

15 Indem der kommerzielle Liberalismus argumentiert, dass Staaten grundlegend immer mehr akzeptieren, dass kriegerische Konfliktlösungsmittel ihren ökonomischen Zielen im Wege stehen, schließt er an dieser Stelle direkt an die Überlegungen des Institutionalismus von Keohane, Nye und anderen an.

2.1.3 Die Rolle nationaler Institutionenarrangements im republikanischen Liberalismus

Im Kontrast zu den beiden bereits vorgestellten Liberalismus-Varianten betrachtet der republikanische Liberalismus die am politischen Willensbildungsprozess beteiligten Institutionen. Für außenpolitische Entscheidungen wurde dabei besonders die Rolle domestischer Institutionen bezüglich eskalativer Tendenzen während Krisen untersucht (Mesquita und Lalman 1990). Deren Rolle bei der Transformation der sozialen Identitäten sowie der beschriebenen wirtschaftlichen Merkmale in tatsächliche Policies steht somit hier im Mittelpunkt (Moravcsik 1997, S. 530). Demokratische und autokratische Staaten könnten durchaus ähnlich gelagerte soziale Identitätsmerkmale sowie wirtschaftliche Strukturen aufweisen, vor allem, falls einer von beiden kürzlich einen Regimewandel durchlaufen hat. Dennoch wäre aufgrund der nunmehr unterschiedlichen institutionellen Ausgestaltung des jeweiligen politischen Systems nicht mehr zwingend auch von ähnlichen politischen Entscheidungen auszugehen. Somit betont der republikanische Liberalismus, dass der Modus der politischen Repräsentativität eine große Rolle bezüglich des letztlichen Staatenverhaltens auf außenpolitischer Ebene spielt. Soziale Gruppierungen artikulieren auch in autokratischen Ländern eigene Präferenzen, jedoch verfügen sie oft nicht über den entsprechenden Zugang zu politischen Positionen und Institutionen, um diese auch in tatsächliche Politikentscheidungen einfließen zu lassen. Politische Institutionen sind laut Moravcsik stets ein Abbild der jeweiligen gesellschaftlichen Gruppe(n), die sie vornehmlich repräsentieren. Ist diese Repräsentation rein exklusiv und auf eine oder wenige Herrschaftseliten zugeschnitten oder beruht sie auf der systematischen Ausgrenzung bestimmter Gesellschaftsgruppierungen vom politischen Willensbildungsprozess, droht eine systematische Ausbeutung des politischen Systems zur Bereicherung der Herrschaftseliten. Die breiten Bevölkerungsschichten in autokratischen Ländern profitieren somit nur selten von den jeweiligen Policys der herrschenden Gruppierung und tragen darüber hinaus oftmals potenzielle Risiken und Verluste an deren Stelle (Moravcsik 1997, S. 530). Die Entwicklungen der letzten Jahre zeigen jedoch für illiberale Demokratien mit vorhandenen Wahlen, dass auch deren politische Repräsentation immer stärker auf Ausgrenzung und der zentralisierten Durchsetzung einzelner Partikularinteressen auf Kosten der Mehrheit der Bevölkerung beruhen kann (Levitsky und Ziblatt 2018). Dieser Aspekt betont somit neben freien und fairen Wahlen gleichzeitig weitere Elemente funktionierender demokratischer Interessenvermittlung, wie sie etwa im Konzept der ›*Embedded Democracy*‹ zum Ausdruck kommen (Zivilgesellschaft, politische und zivile Freiheiten, horizontale Verantwortlichkeiten und eine effektive Regierungsgewalt; Merkel 2004, S. 37).

Gemäß der liberalen Grundannahme, soziale Gruppierungen seien prinzipiell risikoavers, neigen in erster Linie autokratische Länder zu konfliktivem Verhalten, da hier die EntscheidungsträgerInnen die verbundenen Risiken an die Bevölkerung auslagern können (Keohane 2002, S. 46–47). Andererseits könnten auch die ideellen bzw. kommerziellen Präferenzen der Bevölkerung konfliktiv wirken und eine Ausweitung der politischen Repräsentation könnte somit gerade den gegenteiligen Effekt nach sich ziehen (Moravcsik 1997, S. 531). Nichtsdestotrotz legt der republikanische Liberalismus den analytischen Grundstein für das Theorem des demokratischen Friedens, das als eine Art ›em-

pirisches Gesetz‹ angesehen wird. Zurückgehend auf Immanuel Kants Werk »*Zum ewigen Frieden*«, worin dieser bereits Ende des 18. Jahrhunderts die republikanische Staatsform als die friedensgeneigteste bezeichnete, wird argumentiert, dass BürgerInnen in republikanischen Gesellschaften »*sich sehr bedenken werden, ein so schlimmes Spiel* [den Krieg; Anm. der Autorin] *anzufangen*« (Kant 1795, S. 11). Jedoch sollte damit nicht postuliert werden, dass von Demokratien initiierte Kriege prinzipiell ausgeschlossen seien: Entsprechend der dyadischen Variante des Theorems neigen Demokratien sehr wohl auch zu konfliktivem Verhalten, jedoch in erster Linie gegenüber autokratischen Kontrahenten (Rousseau et al. 1996).[16]

Abbildung 3: Kausalpfad des republikanischen Liberalismus nach Moravcsik

(Eigene Darstellung)

2.2 Das Management asymmetrischer Interdependenzen aus Sicht des neuen Liberalismus: »*Politicians still matter*«

Auch Moravcsik erfasst durch seine Konzeption konfliktiver vs. kooperativer Präferenzkonstellationen deren Interdependenzen innerhalb eines Staates sowie die Interdependenzen zwischen den Außenpolitiken verschiedener Staaten. Nach seinen Ausführun-

16 Partielle historische Ausnahmen hiervon im Sinne zwischendemokratischer Kriege finden sich bei Russett 1994, S. 17. Generell kann zwischen einer kulturell-normativen, sowie strukturell-institutionellen Erklärungsvariante des Liberalismus für den demokratischen Frieden unterschieden werden. Postulierte demokratische Charakteristika, wie die öffentliche Kontrolle der Regierung durch das Parlament, die Opposition sowie die Öffentlichkeit, seien speziell in sicherheits- und außenpolitischen Fragestellungen jedoch aufgrund der Dominanz der Exekutive nur eingeschränkt wirksam, was aus Sicht der Liberalen den Befund von demokratisch initiierten Kriegen ohne zugrunde liegender Bedrohung rechtfertigen könne (Schimmelfennig 2013, S. 220–221). Der hierbei zudem entscheidende Aspekt der gesteigerten Geheimhaltung im Bereich der Sicherheitspolitik wird nochmals explizit für den Cyberspace aufgegriffen.

gen erscheinen nationale Regierungen in diesem Gefüge jedoch weitgehend als passive KonsumentInnen der innerstaatlichen Interessenaggregation, die sie ungefiltert in Außenpolitik transferieren. Ein Eigeninteresse demokratischer und autokratischer Regierungsträger ist demnach hier nicht angelegt. Wird jedoch bedacht, dass nationale Regierungen vor allem demokratischer Staaten, stets unter dem Eindruck der nächsten Wahlen, mit einer Vielzahl an unterschiedlichen Partikularinteressen nach innen sowie anderen Staaten und deren Präferenzen auf internationaler Ebene konfrontiert werden, scheint ein gewisses staatliches Management dieser Präferenzinterdependenzen geradezu unausweichlich zu sein. Dieses erfordert zwar nicht zwingend ein autonomes inhaltliches Interesse nationaler Regierungen, jedoch einen hinreichend autonom-strategischen Handlungsspielraum politischer AkteurInnen gegenüber beiden Politikebenen.

Der neue Liberalismus inkludiert, wie beschrieben, Policy-Interdependenzen als Nexus zwischen domestischer Präferenzbildung und dem letztlichen Staatenverhalten. Um noch genauer konzeptualisieren zu können, wann sowohl von demokratischer als auch autokratischer Seite Cyberproxys eingesetzt werden, um den eigenen Handlungsspielraum gegenüber dominanten domestischen Präferenzen, die jedoch inkompatibel zu denen anderer Staaten sind, zu erweitern, wird im Folgenden auf Elemente des neoliberalen Institutionalismus zurückgegriffen. Dessen Unterscheidung zwischen Vulnerabilität und Sensitivität ermöglicht es, die Beschaffenheit und Salienz unterschiedlicher Policy-Interdependenzen analytisch zu erfassen und somit im Folgenden argumentieren zu können, welche Rolle Cyberproxys dabei spielen können. Im weiteren Verlauf wird somit aufgezeigt, warum gerade Cyberproxys, trotz des Primats gesellschaftlicher Präferenzbildungsprozesse zur Erklärung außenpolitischen Verhaltens, demokratischen und autokratischen Regierenden das Management asymmetrischer Interdependenzsituationen erlauben.

2.2.1 Verhandlungsmacht nach innen und außen

Der Liberalismus versteht unter *Macht* die Interessensdurchsetzungschancen der dominanten innerstaatlichen AkteurInnen im Rahmen domestischer und internationaler Aushandlungsprozesse. Domestische AkteurInnen, die ihre Präferenzen effektiver auf die politische Agenda transportieren können, verfügen über eine größere Macht als solche ohne einen entsprechenden Zugang zum politischen System. Durch Wahlen ist der Theorie nach in demokratischen Gesellschaften den BürgerInnen ein Mindestmaß an Zugang zu politischen Entscheidungen garantiert. Im Hinblick auf das politische Tagesgeschäft unterscheiden sich die jeweiligen Interessensdurchsetzungschancen gesellschaftlicher Gruppen jedoch zwangsläufig erheblich und können kontextabhängig signifikant variieren (Palm und Schulz 2011). In autokratischen Staaten ist der Transmissionsriemen verkürzt bzw. defizitär, da ein Großteil der BürgerInnen hierdurch nicht repräsentiert wird. Somit kommt der jeweiligen Herrschaftselite in solchen Gesellschaften ein noch größeres Maß an Macht im liberalen Sinne zu als in demokratischen Ländern, da

hier die politische Repräsentation verfassungstheoretisch und/oder verfassungswirklich auf einzelne Teile der Winning Coalition beschränkt bleibt.[17]

Der neoliberale Institutionalismus unterscheidet die Salienz der Interdependenzbeziehungen anhand zweier Konzepte: *Sensitivität* und *Vulnerabilität.*[18] Darin angelegt ist eine implizite Bewertung der staatlichen Handlungsoptionen im Rahmen der jeweiligen Interdependenzsituation, um etwaige Kosten daraus langfristig vermeiden zu können und somit den eigenen Handlungsspielraum zu vergrößern. Da Cyberproxys als solche Handlungsoptionen konzeptualisiert werden, werden die beiden Konzepte nachfolgend (unter Punkt 2.2.2) für den Cyberspace als Konfliktaustragungsraum erläutert. Ferner wird aufgezeigt, wie sich deren Ausprägungen zu Gunsten demokratischer sowie autokratischer EntscheidungsträgerInnen modifizieren lassen.

Als zweite Modifizierung/Erweiterung des neuen Liberalismus wird zudem die Grundannahme des Zwei-Ebenen-Spiels von Putnam integriert, die besagt, dass vor allem demokratische EntscheidungsträgerInnen stets beide Verhandlungsebenen, die domestische sowie die internationale, zugleich berücksichtigen und bespielen müssen. Gleichzeitig können sie jedoch auch variante Interessensdurchsetzungschancen auf der einen Ebene zu einer effektiveren Zielerreichung auf der anderen nutzen (Putnam 1988, S. 433–435). Somit kann der stärker ausgeprägte Transmissionsriemen demokratischer Staaten zwar theoretisch den Handlungsspielraum demokratischer Regierungen nach innen beschränken, ihnen jedoch gleichzeitig entsprechend der Metapher der ›Tying Hands‹ eine vorteilhaftere Ausgangsposition auf internationaler Ebene liefern.[19] In vorliegender Arbeit wird dieser Gedanken aufgegriffen, da er die theoretische Begründung dafür liefert, wie politische EntscheidungsträgerInnen auch in demokratischen Staaten strategisch autonom handeln können, um unter der Bedingung zunehmender Policy-Interdependenzen aus ihrer Sicht die domestischen Präferenzen so rational wie möglich umzusetzen.[20] Ferner dient der Zwei-Ebenen-Ansatz als eine Art Verbindungsglied

17 »*Winning Coalitions*« werden entsprechend der Selektoratstheorie von Bueno de Mesquita et al. als der Teil des Selektorats beschrieben, dessen Unterstützung für das jeweilige Regime unerlässlich ist, um im Amt zu bleiben, im Austausch für spezielle Privilegien (2005, S. 11). Daher ist die Winning Coalition in Demokratien gemeinhin weitaus größer als in Autokratien, da die Unterstützung größerer Teile der Bevölkerung zur Widerwahl nötig ist, als in Autokratien. Im Rahmen dieser Arbeit wird der Ausdruck somit nicht nur für Autokratien verwendet, sondern auch für die in Demokratien als zentral erachteten Interessensgruppen, deren Einfluss auf die nationale Cyberproxy-Nutzung untersucht wird.

18 An dieser Stelle ist ebenfalls die von Keohane und Nye herausgestellte Unterscheidung zwischen Interaktionen mit und ohne signifikanten Kosteneffekten bedeutsam. Nur im ersten Falle könne auch von »*interdependencies*« gesprochen werden. Interaktionen ohne enthaltene Kosten für beide beteiligte Parteien seien somit eher als »*interconnectedness*« zu bezeichnen (Keohane et al. 2012, S. 8).

19 So könnte eine demokratische Regierung im Rahmen internationaler Verhandlungen auf die Stärke unterschiedlicher Vetospieler im eigenen politischen System verweisen, deren Ratifikation international ausgehandelter Verträge auf domestischer Ebene zwingend notwendig ist.

20 Die Annahme, staatliche AkteurInnen handelten generell rational, kann natürlich kritisiert werden. Es wird an dieser Stelle jedoch im Sinne der »*Bounded Rationality*« argumentiert. Diese »*is used to designate rational choice that takes into account the cognitive limitations of the decision-maker – limitations of both knowledge and computational capacity. Bounded rationality is* […] *deeply concerned with the ways in which the actual decision-making process influences the decisions that are reached*« (Simon

zwischen neuem Liberalismus und neoliberalem Institutionalismus: In der vorliegenden Arbeit wird weder die domestische Präferenzbildung noch die Wirkung als gegeben angenommener Interdependenzen auf internationaler Ebene ausschließlich erfasst. Stattdessen wird eine Verschränkung beider Aspekte angestrebt, um ein theoretisch fundiertes Cyberproxy-Erklärungsmodell zu entwickeln und zu testen.

2.2.2 Sensitivität und Vulnerabilität im Cyberspace

Keohane und Nye trugen mit ihrem Werk »*Power and Interdependence: World Politics in Transition*« maßgeblich zur Etablierung des Konzeptes der Interdependenz auch auf sozialwissenschaftlich-analytischer Ebene bei. Darin sahen die Autoren jedoch nicht nur ein formales Analysekonzept, sondern befürworteten eine bewusste ›Politics of Interdependence‹, damit Staaten vor allem von den postulierten wirtschaftlichen Vorteilen (Abbau von Handelshemmnissen, Arbeitsteilung, Skaleneffekten etc.) profitieren könnten (Spindler 2014, S. 59). Um deren Auswirkungen noch fundierter untersuchen zu können, prägten sie die Konzepte der Sensitivität und Vulnerabilität. Erstere bezieht sich dabei auf die zumeist kurzfristigen Auswirkungen wechselseitiger Abhängigkeiten in einer Situation, in der die politischen Strukturen unverändert bleiben und keine Policy-Anpassungen vorgenommen werden (können), um potenzielle Kosten dieser Interdependenzsituation reduzieren zu können (Keohane et al. 2012, S. 10).

Die Vulnerabilität einer Interdependenzbeziehung beschreibt laut Keohane und Nye dagegen eine Situation, in der deren Kosten durch (auch kurzfristige) Policy-Maßnahmen verändert werden können. Staaten mit einer geringen Vulnerabilität innerhalb der jeweiligen Interdependenz sind nun nicht mehr ›gefangen‹ in ihren jeweiligen Policy-Settings, sondern können auf Handlungen ihres Gegenübers auf politischer Ebene reagieren und somit potenzielle Kostensteigerungen abfedern.[21] Ein Staat kann in einer Interdependenzsituation somit zwar sensitiver, gleichzeitig jedoch weniger vulnerabel gegenüber externen Veränderungen sein als sein Konterpart.[22] Hierfür könnten vor allem dessen »*political will, governmental ability, and resource capabilities*« verantwortlich sein (Keohane et al. 2012, S. 13).

Handlungen im Cyberspace können die Sensitivität und Vulnerabilität von Interdependenzbeziehungen für Staaten erheblich beeinflussen.[23] Digitale Infrastrukturen und Technologien nehmen sowohl in demokratischen als auch zunehmend in autokratischen Ländern immer bedeutendere Positionen ein. Durch die Digitalisierung veränderte sich auch die liberale Strukturbedingung der Globalisierung entscheidend. Die Handlungen

---

1972). Proxies werden somit auch als Mittel von Regierungen angesehen, um die Rationalität von Dritten, wie nationalen Bevölkerungen oder anderen Regierungen, durch das Vorhalten oder Manipulieren von Informationen bewusst beeinflussen zu können.

21 Andrew Moravcsik würde hier von einer geringeren ›Präferenzintensität‹ sprechen.

22 »[…] *the ability of the less vulnerable to manipulate or escape the constraints of an interdependent relationship at low cost is an important source of power*« (Keohane und Nye Jr 1998, S. 86).

23 Wie Keohane und Nye auch, stellt die vorliegende Arbeit das Konzept der Vulnerabilität klar in den Vordergrund, da der bereits bei Moravcsik angelegte Handlungsspielraum politischer AkteurInnen durch dessen Erweiterung im Sinne der Proxy-Nutzung in den Mittelpunkt gerückt wird.

einzelner Staaten unterliegen hiermit nicht mehr nur steigenden Policy-Interdependenzen, wobei im Falle einer globalisierten, nicht aber digitalisierten Welt nationale Grenzen und Jurisdiktionen und somit letztlich die staatliche Hoheitsgewalt jedoch weitgehend intakt geblieben sind. Stattdessen bedingte das zunehmende Maß an digital basierter Kommunikation, Transaktion und Interaktion durch die dezentrale und auf Anonymität ausgerichtete Grundstruktur des Internets, dass diese traditionelle Souveränitätskonzeption für Staaten nur noch eingeschränkt Geltung im Sinne einer »*Cyber-Westphalia*« entfalten kann (Demchak und Dombrowski 2013).[24] Eine Art Folgeabschätzung der Auswirkungen der eigenen Präferenzdurchsetzung auf internationaler Ebene sowie möglicher Rückkopplungseffekte erscheint im Cyberspace noch bedeutend schwieriger. Dies betrifft vor allem auch offensive Cyberoperationen mit besonders schwerwiegend disruptiver Intention: Diese bergen aus staatlicher Sicht stets die Gefahr unkontrollierter Kollateralschäden für die eigene Bevölkerung und Wirtschaft. Nationale Banken sind durch das System der ›Society for Worldwide Interbank Financial Telecommunication‹ (SWIFT) so stark miteinander vernetzt, dass ein Angriff auf einzelne Teile stets auch die eigenen FinanzakteurInnen betreffen könnte. Das realistische Argument, Staaten mit dominanten Cyberfähigkeiten könnten ihre Interessen durch deren machtpolitische Anwendung somit in jedem Falle durchsetzen, greift durch diese Form der digitalisierten Interdependenz somit nur eingeschränkt. Dennoch könnten Staaten, die einen hohen Anteil der digitalen Infrastruktur auf internationaler Ebene de facto unter ihrer Kontrolle/Verwaltung haben, andere Staaten durch diese technologische Monopolstellung in gewisser Weise von sich abhängig machen. Die Folge könnte eine hegemoniale Interessendurchsetzung gegenüber technisch abhängigen Verbündeten oder eine Art Counter-Balancing Dritter durch den Aufbau paralleler Infrastrukturen sein. Der technische Kapazitäts- und Machtaufbau ist im Cyberspace weitaus weniger an territoriale Zuständigkeiten und Befugnisse gebunden. Während ein Land für das Stationieren eigener Seestreitkräfte im Ausland dessen Erlaubnis benötigt, sind Betrieb und Kontrolle der zentralen Root-Nameserver,[25] die überwiegend in den USA und Europa stationiert sind, hiervon nicht abhängig. Die USA hielten lange über die Mandatierung der ICANN[26] de facto Prärogativrechte im Bereich der Verwaltung des für das Internet zentralen Domain Name Systems (DNS) und konnten somit erheblichen Einfluss auf die internationale Regulierung des Internets nehmen. Das Routing wurde jedoch speziell durch die Anwendung der Methode Anycast dezentralisierter, hinzu kam die Abgabe der IANA-Funktio-

---

24 Als »*Cyber-Westphalia*« wird eine Übertragung des Souveränitätskonzepts von Nationalstaaten, welches aus dem Westphälischen Frieden am Ende des Dreißigjährigen Krieges hervorgegangen ist, auf den Cyberspace verstanden. Das Konzept steht somit im Widerspruch zur Annahme, dass der Cyberspace grenzenlos und entterritorialisiert sei. Fragmentierungsbestrebungen staatlicher AkteurInnen gelten dagegen als Versuch, nationale Souveränität ähnlich der analogen Sphäre auch im Cyberspace herzustellen.

25 Ein Root-Nameserver arbeitet an der ›Wurzel‹ (Root) des DNS und ist für die Adressfindung einer Domain verantwortlich (WinTotal 2020).

26 Die ›Internet Corporation for Assigned Names and Numbers‹ ist verantwortlich für die Koordination des Domain Name Systems und die Vergabe von IP-Adressen, der sog. IANA-Funktionen (‚In ternet Assigned Numbers Authority‹).

nen an die ICANN seitens des US-Handelsministeriums 2016, wohl auch eine US-Konzession gegenüber anderen Staaten in Folge der NSA-Affäre.[27]

Nichtsdestotrotz können auch Cyberoperationen selbst eine staatliche Strategie darstellen, um eine Art Vulnerabilitäts-Linkage zu kreieren: Indem die Verwundbarkeit eines Gegenübers durch eine Cyberoperation ausgenutzt wird, kann die eigene Verwundbarkeit in einem anderen Sachbereich verringert werden. Der tatsächliche Erfolg dieser Strategie kann dabei oftmals nur schwer bewertet werden. Wichtig ist im Sinne der Bounded Rationality, dass der jeweils staatliche Akteur diese Strategie als zielführend erachtet, auch unter den einschränkenden Bedingungen einer nur unzureichenden Informationslage. Cyberproxys werden somit durch ihren offensiven sowie defensiven Einsatz als strategische Handlungsoptionen autokratischer und demokratischer Regierungen angesehen, um entweder den Zustand der unvollständigen/unkorrekten Information beim Gegenüber aufrechtzuerhalten und/oder gleichzeitig die Auswirkungen der eigenen, defizitären Informationslage besser managen zu können. Hierdurch wird jeweils die eigene Verwundbarkeit in einem anderen Bereich (z.B. im Falle von Autokratien auf konventioneller militärischer Ebene) oder auf Cyberebene selbst (z.B. im Falle von Demokratien aufgrund ihrer stärkeren Vernetzung) verringert. Die nachfolgenden Ausführungen sollen empirisch verdeutlichen, was das für die Konzepte der Vulnerabilität und Sensitivität im Cyberspace bedeutet.

Operationen im Cyberspace können einerseits dazu führen, dass die Sensitivität eines Landes im Rahmen einer analogen Interdependenzbeziehung ansteigt, für den Fall, dass keine Policy-Anpassungen vorgenommen werden (können). Ein Beispiel wäre die wirtschaftliche Interdependenzbeziehung zwischen zwei Ländern, in der eines der beiden geistiges Eigentum des anderen mithilfe von Cyberspionage stiehlt. Hierbei kann die Sensitivität des bestohlenen Landes hoch sein. Die Kosten der Interdependenzbeziehung könnten insofern steigen, als sich der angreifende Staat im Sinne des ›leapfrogging"[28] unverhältnismäßige Vorteile auf technologischer Ebene verschafft hat und in der Folge weniger abhängig von Importen des anderen Staates in diesem Bereich ist. Die analoge Asymmetrie der Beziehung wurde somit ausgeglichen oder vielleicht sogar auf längere Sicht umgekehrt. Die beschriebene Situation betrifft in erster Linie die Sensitivität des (wahrscheinlich zumeist demokratischen) Opferlandes in Folge einer (wahrscheinlich zumeist autokratischen) Cyberoperation.[29] Ob der ausspionierte Staat jedoch auch eine hierdurch erhöhte Vulnerabilität aufweist, hängt von dessen Reaktionsoptionen ab.

Ein zweites Szenario bezieht sich auf den Fall, dass ein autokratischer Staat Cyberoperationen gezielt dafür nutzt, um seine eigene Vulnerabilität im Rahmen einer Interdependenzsituation mit demokratischen Staaten zu verringern, und im Ergebnis eben-

27 Dennoch ist die US-Regierung auch seitdem Teil des ›Governmental Advisory‹ Committee der ICANN und verfügt somit über bedeutende Veto-Rechte, trotz der Abgabe der IANA-Funktionen (Ermert 2016).

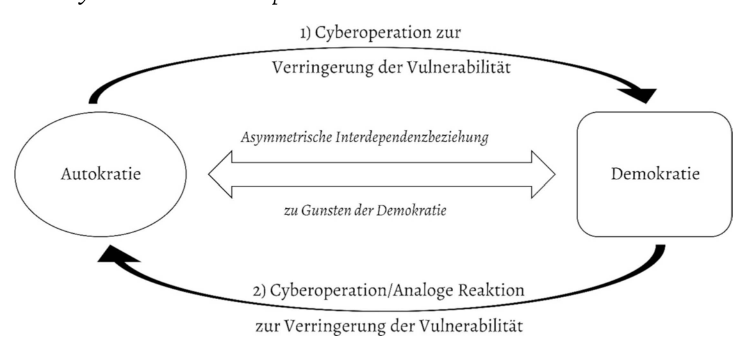
28 Dies bezeichnet das Überspringen einzelner Stufen bei der Entwicklung neuer Technologien.

29 Der bisherige Forschungsstand spiegelt die Annahme wider, dass vor allem autokratische Staaten offensiv im Cyberspace agieren und wie im Falle Chinas den technologischen Vorsprung vor allem demokratischer Staaten durch Cyberspionage versuchen aufzuholen (Gilli und Gilli 2019).

falls eine gestiegene Sensitivität auf demokratischer Seite hervorruft. Hat beispielsweise eine wirtschaftlich aufstrebende Autokratie bereits hinlänglich versucht, durch analoge Maßnahmen (wie dem Anwerben ausländischer WissenschaftlerInnen) die für sie negative asymmetrische Interdependenzbeziehung zu einem demokratischen Technologieführer zu verringern, könnte als effektiveres Mittel folglich die beschriebene Cyberspionage eingesetzt werden. Hierdurch könnte die eigene Vulnerabilität innerhalb dieser Beziehung verringert werden, etwa für den Fall, dass besagte Demokratien es ihren eigenen BürgerInnen erschweren, im Ausland für staatseigene, autokratische Unternehmen zu arbeiten (Bartlett 2020). Erfolgt vonseiten der Demokratie daraufhin keine Reaktion auf der Policy-Ebene, kann dies wiederum zu einer kurzfristig erhöhten Sensitivität führen. Um hieraus jedoch keine längerfristige Vulnerabilität werden zu lassen, könnten nun analoge Maßnahmen, etwa Strafzölle oder Sanktionen, aber auch Gegenschläge im Cyberspace eingesetzt werden. Aufgrund der hier jedoch oftmals unklaren Ursache-Wirkungs-Zusammenhänge bzw. der häufig angezweifelten Effektivität solcher Maßnahmen im Sinne einer angestrebten Verhaltensveränderung beim Gegner (*Coercion*; s. Valeriano et al. 2018; Borghard und Lonergan 2019) erscheinen analoge Reaktionen in einer solchen Situation oftmals plausibler, nicht zuletzt aufgrund der beschriebenen materialistisch-rationalistischen Kosten entsprechend sophistizierter Cyberoperationen.

Cyberoperationen zur Manipulation asymmetrischer Interdependenzvulnerabilitäten können über unterschiedliche Politikfelder sowie über verschiedene Politikebenen hinweg angestrebt werden (Vulnerabilitäts- oder Issue-Linkage). Sieht sich beispielsweise eine Autokratie auf internationaler Ebene einer asymmetrischen Verwundbarkeit auf ideeller Ebene ausgesetzt, indem ihre internen Repressionsstrategien seitens demokratischer Länder kritisiert und sanktioniert werden, kann sie Cyberoperationen nutzen, um die asymmetrische Verwundbarkeit besagter Demokratien auf domestisch-ideeller Ebene zu ihrem Vorteil auszunutzen, etwa indem bei der Operation die spezifischen Defizite demokratischen Regierens im Vordergrund stehen. Cyberoperationen können somit die Gesamtbilanz der Vulnerabilitätsasymmetrie zwischen zwei Ländern manipulieren.

Abbildung 4: Cyberoperationen zur Verringerung von Vulnerabilitäten im Rahmen asymmetrischer Interdependenzsituationen



(Eigene Darstellung)

2.2.3 Der strategische Handlungsspielraum autokratischer AnführerInnen

Zwar sehen sich autokratische Exekutiven in weitaus geringerem Maße der effektiven Interessensdurchsetzung nichtstaatlicher ziviler AkteurInnen gegenüber, dennoch wollen auch sie gegenüber anderen Akteursgruppierungen existierende Asymmetrien auf domestischer Ebene entsprechend der eigenen Ziele gestalten, um die eigene Führungsposition am Ende des defizitären Transmissionsriemens nicht zu gefährden. Diese ›Manipulationsmöglichkeiten‹ betreffen für autokratische Regime somit in erster Linie das Verhältnis zwischen der Exekutive sowie den sonstigen Herrschaftseliten, die oftmals auch als »Winning Coalition« bezeichnet werden (Mesquita et al. 2005).

2.2.3.1 Asymmetrische Verhandlungsmacht nach innen

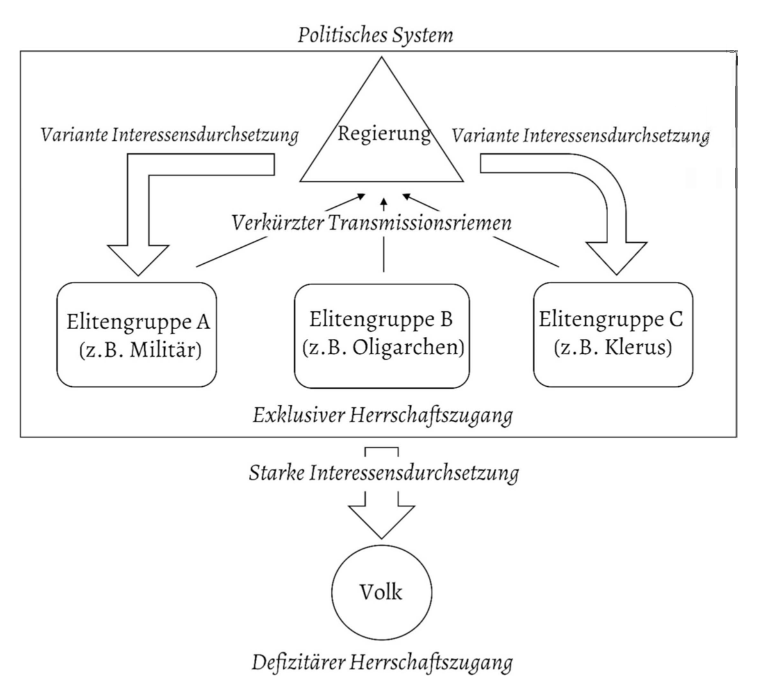
Autokratische Systeme sehen einen breiten Herrschaftszugang für eine kleine Gruppe an AkteurInnen bzw. einen verengten bis kaum vorhandenen Zugang für eine breite Masse vor. Autokratische Regierungen verfügen somit über ein zu ihren Gunsten ausgestaltetes Interessensdurchsetzungspotenzial gegenüber der Bevölkerung. Die Interessen der politischen Eliten sind in Autokratien wesentlich schwächer an die der breiten Bevölkerung gekoppelt als in Demokratien. Fehlende oder manipulierte Wahlen sowie weitere Einschränkungen der Elemente einer konsolidierten Demokratie, etwa des Wirkens der Zivilgesellschaft, sind hierfür als Gründe zu nennen.

Dennoch sind auch in Autokratien verschiedene Elitengruppierungen nochmals mit varianten Herrschaftszugängen und somit auch unterschiedlichen Interessensdurchsetzungschancen gegenüber der Regierung ausgestattet. Hierfür hauptverantwortlich gemacht werden die divergierenden, autokratischen Legitimationskonzeptionen verschiedener autokratischer Subregimetypen (z.B. Militärregime oder Monarchien), die die Kooptation und/oder Repression unterschiedlicher gesellschaftlicher Gruppierungen erforderlich machen. Die Begriffe *Kooptation* und *Repression* entstammen der Terminologie zur Forschung über autokratische Stabilisationsmechanismen (Gerschewski 2013). Im Sinne liberaler Theorien beschäftigt sich diese Forschung damit, wie autokratische HerrscherInnen sicherstellen können, dass trotz fehlenden Herrschaftszugangs im Sinne freier und fairer Wahlen sowie eingeschränkter sonstiger Repräsentations- und Partizipationsrechte der breiten Bevölkerung durch das Zusammenwirken dreier Säulen ein Stabilisierungsmechanismus zur Festigung der Regierungsposition etabliert werden kann.[30] Dies stellt gleichzeitig die theoretische Überleitung zu den drei Spielarten des Liberalismus nach Moravcsik dar: Die drei Säulen autokratischer Stabilität von Gerschewski, Repression, Kooptation und Legitimation, lassen sich direkt an eine oder mehrere dieser Theorievarianten anknüpfen. Autokratische Cyberproxy-Operationen werden in der vorliegenden Arbeit jedoch in erster Linie im Hinblick auf die Säule der

30 »*Instruments of representation include formal representation, constitutional structure, informal institutional dynamics, appointment to government, and the organizational capacity of social actors. By changing the »selectorate«– the individuals and groups who influence a policy – the policy changes as well*« (Moravcsik 2013, S. 5). Somit könnten etwa auch Bestrebungen demokratischer Parteien, das Wahlrecht zu Gunsten ihrer Stammwählerschaft zu verändern, eine solche Veränderung des Selektorats und somit der sich durchsetzenden Politik bedeuten.

Legitimation analysiert, wenngleich deren repressiven Potenziale ebenfalls diskutiert wurden (z.B. Deibert 2009; Deibert 2015; Gunitsky 2015).

Abbildung 5: Asymmetrische Verhandlungsmacht autokratischer Regierungen nach innen



(Eigene Darstellung)

Seitens der Regimeforschung wurde die Thematik der Legitimation im autokratischen Kontext lange vernachlässigt. Die Annahme lautete, dass aufgrund des fehlenden demokratischen Wahlmechanismus von vornherein lediglich Repression und Kooptation als Mittel des Herrschaftserhalts gewählt würden (s. Burnell 2006; Grauvogel und Soest 2014). Forschungsarbeiten der letzten Dekade zeigten jedoch besonders im digitalen Kontext, dass auch autokratische AnführerInnen auf eine gewisse Form von Legitimation angewiesen sind, um ihre Stellung im politischen System zu behaupten (Morozov 2011; King et al. 2013; Rød und Weidmann 2015; Göbel 2015).[31] Autokratische

31 Aufgrund des omnipräsenten Damoklesschwertes autokratischer Kontrolle und Repression besteht hierbei jedoch stets die Gefahr einer antizipativen Selbstzensur der Bevölkerung, was somit den Nutzen solcher Maßnahmen zur Überwindung des Dictator's Dilemma schwächt (Gueorguiev et al. 2018).

Legitimation kann sich dabei aus verschiedenen Quellen speisen: aus der diffusen oder spezifischen Legitimität der politischen Institutionen und deren Handlungen.[32]

Das Fehlen oder die inhaltliche Korrumpierung rechtsstaatlicher und demokratischer Strukturen macht einerseits einen alternativen Modus der Herrschaftssicherung notwendig und ermöglicht andererseits dessen nichtdemokratische Prägung. Dem Aspekt der Legitimation kommt dabei auch im Cyberspace eine besondere Bedeutung zu, da er zu stärkeren oder schwächeren Vulnerabilitäten des Regimes auf allen drei Liberalismusebenen führen kann, durch diese aber auch entscheidend beeinflusst wird. Eine Autokratie mit hinreichendem Reichtum an natürlichen Bodenschätzen könnte aufgrund dieser schwächeren Präferenzintensität bzw. Verwundbarkeit gegenüber externen Rohstoffimporten daher auch eher auf eine Output-orientierte Legitimationskonzeption setzen. Dies wäre jedoch im Einzelfall zu überprüfen.

Nach innen besteht somit zumeist ein aus Sicht der autokratischen Führung zu ihren Gunsten asymmetrisches Interdependenzverhältnis gegenüber der breiten Bevölkerung. Inwiefern dies jedoch auch auf die Beziehung zu systemrelevanten Elitengruppen zu trifft, ist eine spezifische Subtypen-Frage.

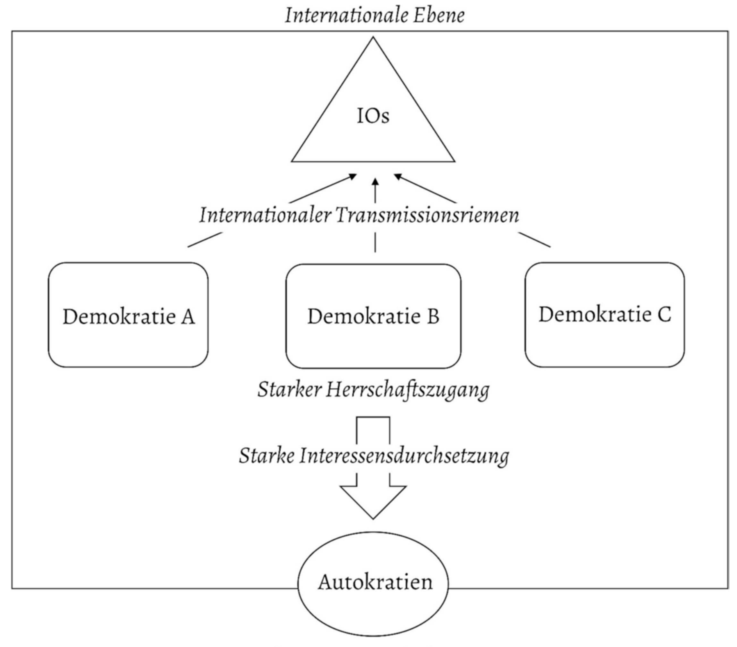
2.2.3.2 Asymmetrische Verhandlungsmacht nach außen

Auf zwischenstaatlicher Ebene ist die Asymmetrie der Interessensdurchsetzungspotenziale zumeist zum Nachteil der Autokratien ausgeprägt. Dies bezieht sich nach wie vor besonders auf die militärische Ebene, etwa wenn eine Autokratie selbst keine Nuklearwaffen besitzt, ihr demokratischer ›Gegner‹ jedoch schon. Zum anderen ist auch oftmals im konventionellen Bereich eine militärische Unterlegenheit gegenüber demokratischen Staaten bzw. deren affiliierten Militärbündnissen wie der North Atlantic Treaty Organization (NATO) gegeben (Tsygankov 2019, 73, 78). Auf internationaler Ebene setzt sich diese Asymmetrie im Rahmen liberal-demokratisch geprägter internationaler Organisationen überwiegend fort, da diese aus republikanischer, ideeller sowie kommerzieller Sicht zumeist auch den (kapitalistischen) Interessen demokratischer Staaten entsprechen (Cooley 2015, S. 50). Gemäß dem institutionalistischen Paradigma wurden somit internationale Organisationen (IOs) dazu geschaffen, um die Kosten der steigenden Interdependenzbeziehungen zwischen Staaten zu reduzieren, und waren inhaltlich zumeist durch demokratische Prinzipien geprägt (Keohane und Martin 1995). Der Herrschaftszugang demokratischer Staaten war und ist IOs wie den Vereinten Nationen (UN/UNO), der Weltgesundheitsorganisation (WHO) oder der Welthandelsorganisation (WTO) oftmals stärker als der vieler Autokratien. Jedoch lässt sich hierbei auch

32 Erstere bezieht sich dabei auf eine prinzipielle Zustimmung zur Regierung, unabhängig von ihrer tatsächlichen Leistung in Bezug auf sozioökonomische Kennzahlen. Es geht einzig darum, eine Sache (in diesem Fall die Regierung) zu unterstützen, auf Grundlage dessen, was diese ist und repräsentiert und nicht auf der Basis ihres tatsächlichen Verhaltens (Easton 1975, S. 444). Im Gegensatz dazu basiert spezifische Regime-Unterstützung auf der Bewertung der Leistung der Regierung, wie etwa dem allgemeinen Wohlstandsniveau des Landes. Dabei kann sich die Zufriedenheit der BürgerInnen entweder aus konkreten Handlungen der staatlichen Administrationen, oder aber aus einer Bewertung der generellen Performanz der AkteurInnen und Institutionen speisen (Easton 1975, S. 439).

ein gradueller Wandel erkennen: Zum einen streben Autokratien wie China oder Russland seit einigen Jahren die Schaffung eigener regionaler Organisationen an, die ihre Interessen nach außen hin vertreten (z.B. die Shanghaier Organisation für Zusammenarbeit, SOZ). Zum anderen wird denselben Ländern im Rahmen der UN immer wieder attestiert, die dortigen Entscheidungsfindungsprozesse bewusst unterhöhlen zu wollen (Henriksen 2019, S. 3) oder aber – wie im Falle der Internet-Governance – demokratischen Ideen eigene, autokratisch geprägte Normvorstellungen gegenüberzustellen, etwa das Konzept der »*information sovereignty*« (Gechlik 2017, S. 3–4).[33]

Abbildung 6: Asymmetrische Verhandlungsmacht autokratischer Regierungen nach außen



(Eigene Darstellung)

Wichtig ist bei der Verhandlungsmacht autokratischer Staaten nach außen zudem, inwiefern sie durch ihre Stellung gegenüber den beschriebenen internen Elitengruppen in ihrem Handeln bestärkt oder beschränkt werden. Autokratien können im Rahmen eines Zwei-Ebenen-Spiels oftmals glaubhafter als Demokratien versichern, dass sie ihre Forderungen auch gegen den Widerstand domestischer AkteurInnen durchsetzen können, da die Regierung gegenüber der breiten Bevölkerung geringeren politischen

33 Der tatsächliche Erfolg einer vermeintlich geeinten Cybernorm-Förderung autokratischer Staaten wurde jedoch für die SOZ bereits in Frage gestellt (Harnisch 2021).

Verantwortlichkeiten und Rechenschaftspflichten unterworfen ist. Dies kann ihre Interessensdurchsetzungschancen gegenüber anderen Staaten somit potenziell vergrößern. Gemeinhin wurde daher im Rahmen des Zwei-Ebenen-Ansatzes für Autokratien davon ausgegangen, dass die domestische Verhandlungsebene aufgrund fehlender öffentlicher Ratifikationspflichten internationaler Verträge eine geringere Rolle spielt als für demokratische Staaten (Schelling 1960, S. 28). Autokratische Regierungen können internationale Verträge aufgrund der zu ihren Gunsten ausgestalteten Interdependenzbeziehung oftmals leichter durchsetzen als demokratische Regierungen.

Hinzu kommt jedoch in jedem Falle, dass der interne Kampf um die Durchsetzung der eigenen Interessen auf domestischer Ebene auch das außenpolitische Handeln einer autokratischen Regierung beeinflussen kann. Aufgrund des fehlenden (freien) Wahlmechanismus als institutionalisierter Nachfolgeregelung erfordert die autokratische ›Coup-Proofing‹-Strategie oftmals, dass autokratische Führer ihre domestischen Interessen gegenüber Elitengruppierungen mit Handlungen der internationalen Ebene verknüpfen, um diese effektiver durchsetzen zu können. Ein hypothetisches Beispiel für den Cyberspace wäre die Unterstützung einer Norm, die Staaten militärisch geführte Cyberoperationen in Friedenszeiten grundsätzlich untersagt. Eine autokratische Regierung, die sich zunehmend ermächtigten Militärs gegenübersieht, könnte deren digitales Coup-Potenzial durch eine Handlung auf internationaler Ebene im Sinne des von Moravcsik für noch nicht konsolidierte Demokratien propagierten »*Lock-in*«-Effekts einschränken (Moravcsik 2000, S. 220).[34] Somit können die Kosten einer internen Interdependenzbeziehungen durch Handlungen auf der außenpolitischen Ebene im besten Falle reduziert werden.

2.2.4 Der strategische Handlungsspielraum demokratischer AnführerInnen

Laut neuem Liberalismus repräsentieren politische Institutionen lediglich die Interessenvertretungen der domestisch dominanten AkteurInnen nach innen und außen. Da der Transmissionsriemen in liberalen Demokratien weitgehend funktioniert, ist hier auch von einem geringeren Eigeninteresse bzw. autonomen Handlungsspielraum der PolitikerInnen auszugehen, was den dominierenden sozialen Interessen zuwiderläuft. Inwiefern diese Annahmen im Rahmen von Interdependenzbeziehungen sowohl nach innen als auch nach außen jedoch notwendigerweise modifiziert werden müssen, wird nun diskutiert.

2.2.4.1 Asymmetrische Verhandlungsmacht nach innen

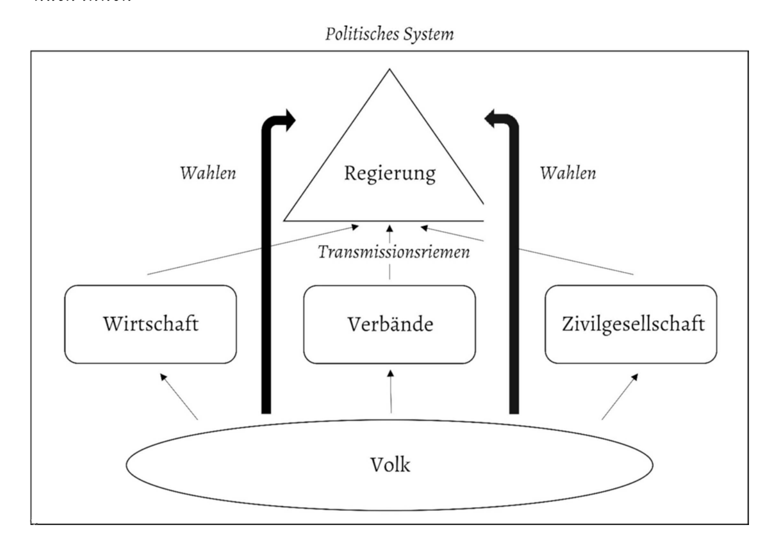
Grundlegend existiert für demokratische Regierungen eine für sie vulnerable, asymmetrische Interdependenzkonstellation auf domestischer Ebene. So müssen sie sich den politischen Herrschaftszugang mit wesentlich mehr AkteurInnen und zudem in einem größeren Umfang teilen als autokratische Regierungen. Der demokratische Wahlmechanismus stellt sicher, dass zumindest alle Wahlberechtigten die prinzipielle Möglich-

34 Hierzu argumentiert Moravcsik, dass »*international institutional commitments, like domestic institutional commitments, are self-interested means of ›'locking in‹ particular preferred domestic policies—at home and abroad—in the face of future political uncertainty*« (Moravcsik 2000, S. 226).

keit haben, durch ihre Stimmabgabe auf die politischen Institutionen und Entscheidungen Einfluss zu nehmen. Gleichzeitig können demokratische PolitikerInnen in der Folge auch an ihren Wahlkampfversprechen gemessen werden. Zudem gilt der Grundsatz ›nach der Wahl ist vor der Wahl‹ – die institutionalisierte Regelmäßigkeit demokratischer Wahlen hat demnach ebenfalls einen Einfluss auf den temporären Herrschaftszugang domestischer Gruppen (Palm und Schulz 2011).

Diese Aspekte haben alle Demokratien weitgehend gemeinsam. Wie im Falle autokratischer Subtypen variieren auch Demokratien jedoch oftmals entlang verschiedener Kriterien. Dies betrifft insbesondere die Ausgestaltung der politischen Institutionen auf der republikanischen Ebene, was auch einen Einfluss auf die wirtschaftlichen Anreizstrukturen sowie die sozialen Identitäten des Landes haben kann. Umgekehrt kann auch ein Wandel auf der ideellen Ebene Veränderungen auf der republikanischen zur Folge haben bzw. zumindest begünstigen. Die Unterscheidung zwischen liberalen und illiberalen Demokratien wird hierbei für die demokratische Instrumentalisierung defensiver Cyberproxys im dritten Kapitel genauer erläutert.[35]

Abbildung 7: Asymmetrische Verhandlungsmacht demokratischer Regierungen nach innen



(Eigene Darstellung)

35 Es existiert noch eine Vielzahl an alternativen Demokratie-Typologien, etwa die auf Jürgen Habermas zurückgehende Unterscheidung zwischen deliberativer und den bereits zuvor existierenden Typen der liberalen und republikanischen Demokratie. Für den theoretischen Ansatz dieser Arbeit wird jedoch der Unterscheidung zwischen liberaler und illiberaler Demokratie ein besonderer Stellenwert im Hinblick auf die unterschiedlichen demokratischen Cyberproxy-Nutzungsmuster zugesprochen, da diese nicht nur die republikanische Ebene des Liberalismus besonders berücksichtigt, sondern auch die beiden anderen Varianten tangiert.

Zusammenfassend ist zu konstatieren, dass Demokratien im Vergleich zu autokratischen Regierungen über eine eingeschränktere politische Autonomie verfügen, da ihre Handlungen durch den existierenden Wahlmechanismus sowie intermediäre Organisationen der Zivilgesellschaft stärker an die Interessen einer breiteren Bevölkerungsschicht angebunden sind. Dies hat zudem laut dem liberalen Theorem des demokratischen Friedens einen besonderen Einfluss auf deren generelle Kriegsaffinität mit noch zu diskutierenden Implikationen für deren Cyberproxy-Gebrauch.[36] Darüber hinaus lassen sich jedoch auch für verschiedene Demokratie-Spielarten unterschiedlich große Handlungsspielräume nach innen feststellen, wie anhand der Unterscheidung zwischen liberalen und illiberalen Demokratieformen im Rahmen des demokratischen Cyberproxy-Gebrauchs noch dargestellt werden wird.

2.2.4.2 Asymmetrische Verhandlungsmacht nach außen

Im Gegensatz zu autokratischen Regierungen kann aufgrund der besonders seit dem Ende des Kalten Krieges Anfang der 1990er Jahre andauernden Dominanz demokratischer Staaten auf internationaler Ebene auch hier von einem größeren Herrschaftszugang gesprochen werden. Das Interdependenzverhältnis zwischen den beiden Lagern war bislang somit stärker zugunsten demokratischer Staaten ausgestaltet. Unter Führung der USA entwickelten diese nach und nach IOs, die ihre eigenen ideellen Wertvorstellungen und Prinzipien widerspiegeln sollten. Mitentscheidend hierfür waren IOs wie die WTO, die aus institutionalistischer Sicht Staaten größere Anreize für wirtschaftliche Kooperation und weniger Anreize für betrügerisches oder konfliktives Verhalten auf internationaler Politikebene lieferten. Der ›zivilisierenden‹ Wirkung der IOs widersprachen in der Folge jedoch auch diverse empirische Beispiele wie die Bürgerkriege in Ruanda und dem Kosovo, die die Schwächen der einheitlichen Beschlussfindung zur Verregelung von Konflikten auf internationaler Ebene verdeutlichten (Seybolt 2007, S. 1). Die ideellen Identitäten der Staaten waren oftmals zu unterschiedlich ausgeprägt, sodass die Entschlussfindung behindert wurde. Gleiches wird auch als Grund für das nach wie vor geringe Verregelungsniveau des Cyberspace auf internationaler Ebene benannt, manifestiert in der ideell geprägten Debatte um ›Information-Security‹ vs. ›Cyber-Security‹ (Hansel et al. 2018).

Im Rahmen des Zwei-Ebenen-Spiels unterliegen demokratische EntscheiderInnen anderen domestischen Restriktionen als autokratische PolitikerInnen. Einerseits sind sie stärker an demokratische Ratifikationserfordernisse im Falle internationaler Verträge gebunden, was ihren Verhandlungsspielraum gegenüber anderen Staaten erheblich einschränken kann. Andererseits können Demokratien diese domestische Restriktion ihres außenpolitischen Handlungsspielraums gezielt zu ihren eigenen Gunsten nutzen, indem sie sich der angesprochenen Strategie der ›*Tying Hands*‹ bedienen. Der scheinbar

---

36 Der u.a. von Oneal and Russet 1997 vertretenen Vorstellung, der demokratische Regimetyp habe direkte und indirekte Auswirkungen auf die Konfliktaffinität demokratischer Staaten, setzt Gartzke 2000 eine noch stärker auf den Kern des neuen Liberalismus ausgerichtete Erklärung entgegen: So ließen Präferenzübereinstimmungen Staaten unabhängig vom Regimetyp regelmäßig von Konflikten Abstand nehmen.

kleinere Handlungsspielraum gegenüber stärkeren domestischen AkteurInnen wird somit auf internationaler Ebene in eine größere Verhandlungsmacht umgewandelt.[37]

Zusammenfassend ist festzuhalten, dass demokratische Regierungen bislang auf außenpolitischer Ebene oftmals über größere Interessensdurchsetzungschancen verfügten als ihre autokratischen Gegenüber.[38] Dies trifft besonders auf Situationen zu, in denen demokratisch geprägte IOs involviert waren. Deren durch eine fehlende ideelle Interessenkonvergenz zwischen Demokratien und Autokratien hervorgerufene Blockade wurde in der Vergangenheit jedoch auch erst durch demokratische Entscheidungsprozesse ermöglicht, was bislang oft auch für den Cyberspace galt. Im Hinblick auf die Erklärung demokratischen Cyberproxy-Gebrauchs wird somit auch das verstärkte Unterminieren internationaler Institutionen durch autokratische Staaten von Bedeutung sein, um aufzuzeigen, welche Handlungsoption Proxys dabei auch für Demokratien darstellen können.[39]

2.3 Fazit: Der Cyberspace als regimetypenübergreifende Chance und Herausforderung zugleich

Als Fazit lässt sich feststellen, dass im Falle beider Regimetypen aus liberaler Perspektive das Mischverhältnis zwischen den asymmetrischen Interdependenzbeziehungen auf innen- und außenpolitischer Ebene den strategischen Handlungsspielraum politischer EntscheidungsträgerInnen beeinflusst und damit einhergehend der Modus Operandi der Herrschaftssicherung mitentscheidend für deren jeweilige Politiken ist. Während autokratische Staaten grundlegend über stärkere Interessensdurchsetzungschancen gegenüber einer breiteren, politisch nicht involvierten Akteursgruppe (der Bevölkerung) verfügen, ist der Handlungsspielraum demokratischer Staaten prinzipiell durch die engere Verflechtung der Interessen eines weitaus größeren Elektorats mit dem politischen Entscheidungsprozess deutlich eingeschränkter.

Digitale Technologien beeinflussen die Durchsetzung gesellschaftlicher Präferenzordnungen auf außenpolitischer Ebene im Falle beider Regimetypen immer umfassender. Es ergeben sich dadurch Rückwirkungseffekte auf die strategische Handlungsautonomie der Regierung auch auf domestischer Ebene. Das Erreichen wirtschaftlicher Performanz wird dabei immer schwieriger, ohne sich von besagter Technologie abhängig zu machen. Aufgrund des unterschiedlich ausgeprägten Herrschaftszugangs führt dies bei

---

37 Hinsichtlich der Implementierung international getroffener Beschlüsse wurde im Rahmen internationaler Klimapolitik bereits diskutiert, inwiefern Autokratien aufgrund der größeren Unabhängigkeit von nationalen Interessengruppen internationale Beschlüsse effektiver und schneller auf nationaler Ebene ›durchimplementieren‹ könnten, als weniger autonome Demokratien (Bättig und Bernauer 2009).

38 Eine weitere, weniger dem Liberalismus und stärker dem Sozialkonstruktivismus zu zuordnende Begründung hierfür wäre das Bilden von sog. ›Ingroups‹, bzw. identitären Gemeinschaften, die gemeinsame Wertvorstellungen als Zugehörigkeitskriterium besitzen und sich selbst als ›Freunde‹ und Nichtmitglieder als ›Feinde‹ ansehen. Die nach dem Zweiten Weltkrieg von Demokratien gegründeten IOs wären dann als solche Gemeinschaften zu verstehen (vgl. Oren 1995; Kahl 1998).

39 Auf eine vierte Grafik zur Veranschaulichung wird an dieser Stelle verzichtet.

Demokratien einerseits zu einer Ausweitung der am Politikprozess in diesem Bereich interessierten AkteurInnen, bei Autokratien zu einer möglichen Interessensverschiebung hinsichtlich veränderter wirtschaftlicher Anreizstrukturen. Besonders für liberal-demokratische Staaten stellt der Cyberraum zugleich eine ideell-republikanische Herausforderung dar: Während die eigene Vorstellung von legitimer, demokratischer ›Good Governance‹ ein hohes Maß an politischer Transparenz und Austausch mit der breiten Bevölkerung vorsieht, kollidiert dies mit der technischen Realität im Rahmen konfliktiver Handlungen im Cyberspace. Demokratische Institutionen sollten somit auch in diesem Bereich möglichst transparent agieren, können dies aufgrund der genuinen Besonderheiten des Cyberspace jedoch oftmals nicht (z.B. Attributionsproblem und ›*Covert Actions*‹).[40] Daher haben sich Geheimdienstausschüsse auf republikanischer Ebene als Vermittler etabliert, die die Defizite des Transmissionsriemens in diesem Bereich teilweise reduzieren sollen. Hinzu kommt, dass die institutionalistische Vorstellung von verregelter Interdependenz und somit kooperativer Außenpolitik für den Cyberspace bislang noch nicht in ausreichendem Maße zum Tragen gekommen ist und Staaten somit eigene Wege finden mussten, um ihre jeweiligen Vulnerabilitäten darin zu reduzieren.

Autokratische Regime stehen dagegen auf republikanischer Ebene vor der Entscheidung, bei welchen Elitengruppen sie im Cyberspace den Herrschaftszugang einschränken oder im Sinne des Coup-Proofings erweitern. Mitentscheidend bei diesen Herausforderungen sind jedoch die potenziellen Kosten im Rahmen der existierenden Interdependenzbeziehungen, die durch Handlungen im Cyberspace entstehen oder durch diese gezielt verringert werden können. Dabei entfalten ökonomische Handlungen im Cyberspace zunehmend auch Implikationen für das Sicherheitsempfinden anderer Länder aus militärischer, aber auch ontologischer und damit ideeller Sicht (Farrell und Newman 2019, S. 43). Für den weiteren Verlauf der Arbeit wird auf analytischer Ebene das Konzept der Vulnerabilität von besonderer Bedeutung sein, da rationale AkteurInnen im Cyberspace kaum noch autonom sind und Proxys die dabei entstehenden Interdependenzkosten verringern können, unabhängig von oder bewusst in Konfrontation zu internationalen Verregelungsbemühungen.

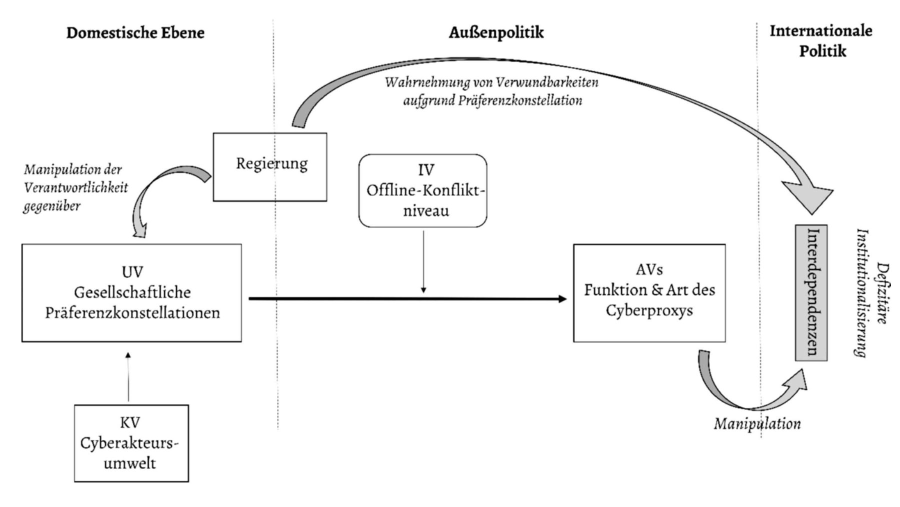
40 Staatliche Maßnahmen im Cyberraum müssen oftmals notwendigerweise geheim gehalten werden, hinsichtlich der Aktionen selbst und/oder des Urhebers (Boeke und Broeders 2018, S. 75).

3. Ein liberales Erklärungsmodell staatlicher Cyberproxy-Strategien

Demokratische und autokratische Regierungen sehen sich – wie aufgezeigt – unterschiedlichen Herausforderungen im außenpolitischen Bereich sowie zunehmender Digitalisierung gegenüber. Der immer grenzüberschreitendere Charakter sozialer, politischer, militärischer sowie wirtschaftlicher Maßnahmen führte dabei zwar zu einer prinzipiellen Kriegsaversion, jedoch gleichzeitig zur immer stärkeren Umkämpftheit aller genannter Domänen, um im globalen Geflecht aus wechselseitigen Abhängigkeiten nicht regelmäßig ins Hintertreffen zu geraten (vgl. Wright 2017). Im Umgang mit diesen asymmetrischen Interdependenzen bedingen – neben der bislang defizitären Institutionalisierung im Cyberbereich – variante Wirkfaktoren auf domestischer Ebene im Sinne ideeller, wirtschaftlicher sowie republikanischer Merkmale regelmäßig unterschiedliche Außenpolitiken. Welche Rolle speziell Cyberproxys für beide Regimearten sowie deren Subtypen im Umgang mit den wahrgenommenen Vulnerabilitätsasymmetrien in interdependenten Präferenzkonstellationen auf außen- und innenpolitischer Ebene zukommt, wird im vorliegenden Kapitel genauer erklärt. Dabei wird zudem erläutert, inwiefern nicht nur die jeweilige inhaltliche Funktion des Proxys ein erklärungswürdiges Phänomen ist, sondern auch dessen institutionelle Anbindung.

Zunächst wird jedoch das Attributionsproblem als asymmetrische Interdependenzsituation behandelt und diskutiert, welche Rolle offensive und defensive Cyberproxys dabei für die jeweiligen Regimetypen spielen können. Darauf aufbauend werden im Anschluss die Variablen des Erklärungsmodells (Abbildung 8) aus Perspektive des neuen Liberalismus konzeptualisiert.

Abbildung 8: Liberales Erklärungsmodell staatlicher Cyberproxy-Strategien



(Eigene Darstellung)

3.1 *Why Cyberproxys Matter:* Das Attributionsproblem als asymmetrische Interdependenzsituation

Besonders im Cyberspace müssen bei der Entscheidung einer Regierung, ob und wie eine Attribution vorgenommen wird, die potenziellen Folgen der Handlung bereits mitgedacht werden. Auch wenn dem Opfer in vielen Fällen der jeweilige Urheber wohl bekannt sein dürfte, bedingen die aufgezeigten Interdependenzen auf allen drei Liberalismusebenen die vermutete Zurückhaltung vor allem demokratischer Regierungen, das Attributionsproblem als Problem der völkerrechtlichen Verantwortungsverregelung und weniger der -identifizierung zu adressieren.[1]

Aus autokratischer Sicht vereinfacht das Internet das Durchführen disruptiver Konfliktmaßnahmen unterhalb der kritischen Gewaltschwelle. Da diese technischen Möglichkeiten bei Zielen mit entsprechenden Attributionskapazitäten jedoch nicht zwingend ausreichen, um eine Identifizierung als Täter zu vermeiden, gilt es, die Bedingungen für demokratische Attributionen zu erschweren bzw. die Kosten hierfür im Rahmen der Interdependenzbeziehung in die Höhe zu treiben. Konkret bedeutet dies, die Rationalitätsgrundlage demokratischen Handelns in Folge einer Cyberoperation durch die (oftmals ambivalente) Kreierung einer Plausible Deniability zu manipulieren.[2] Die Demokratien zur Verfügung stehenden Information sollen dergestalt

1 Experteninterview mit Dr. Brandon Valeriano, Mitglied der US-Cyber-Solarium-Commission, am 28.09.2020.

2 Inwiefern hierbei eher von einer »Implausible Deniability« gesprochen werden sollte, also einer »apparent, but unacknowledged action«, wird besonders für die öffentlichkeitswirksameren russischen Cyberproxy-Operationen von Bedeutung sein. So argumentieren Cormac und Aldrich, dass nur solche Operationen eine *plausibel* abstreitbare *verdeckte* Operation seien, die »neither acknowledged nor apparent« sind, was somit bewusst öffentlich stattfindende Operationen ausklammern

beschränkt bzw. beeinflusst werden, dass diese vor einer direktstaatlichen Attribution zurückschrecken, mit dem Wissen, dass eine Reaktion in Folge einer stets möglichen Fehlattribution potenziell schwere Folgen haben könnte. Der Einsatz von Proxys ist dafür ein geeignetes Mittel, da durch die hiermit geschaffene Informationsasymmetrie die Präsentation umfassender Beweise im Sinne der ›True Attribution‹ sowie die auf rechtstaatlichen Prinzipien basierende Adressierung solcher indirekten Cyberangriffe für demokratische Regierungen erschwert werden. Lässt sich eine staatliche Involvierung lediglich vermuten, jedoch rechtlich nicht einwandfrei belegen, sind die Kosten für eine dennoch erfolgende politische Attribution seitens der Demokratie in Richtung der Autokratie erhöht (Egloff 2020a, S. 61–62). Zudem könnte eine eskalative Reaktion die eigene Verwundbarkeit im Rahmen dieser Interdependenzsituation nicht wie geplant reduzieren, sondern weiter erhöhen. Somit stellte bislang aus autokratischer Sicht das Verbleiben unterhalb der kritischen Gewaltschwelle im Cyberspace eine Art Versicherung dar, die es erlaubte, mithilfe von Cyberoperationen negativ asymmetrische Interdependenzverhältnisse gegenüber Demokratien in der konventionellen Sphäre zu manipulieren (vgl. Tsygankov 2019, S. 164). Zusammenfassend kann somit konstatiert werden, dass Autokratien ihre geringere Vulnerabilität im Rahmen der asymmetrischen Attributionsinterdependenzsituation instrumentalisieren, um mithilfe von Proxys ihre höhere Verwundbarkeit in anderen Interdependenzbeziehungen zu verringern (Vulnerabilitäts-Linkage).

Aus demokratischer Perspektive ist nicht die Täterbeschreibung autokratischer ›Cyber-Rogue-States‹ per se das Problem, sondern die Entscheidung, ob dies öffentlich kommuniziert wird und wie entsprechend im weiteren Verlauf darauf reagiert werden soll (s. Abbildung 9).

Abbildung 9: Die Strategiewahl der Opfer von Cyberoperationen

(Eigene Darstellung basierend auf Baram und Sommer 2019, S. 202)

würde (2018, S. 482). Laut Carson und Yarhi-Milo nutzen Staaten zudem »covert action to convey intentions and coerce adversaries« (2017, S. 124), was besonders für den offensiven Proxy-Gebrauch autokratischer Staaten von Relevanz sein könnte. Auf demokratischer Seite steht dagegen im Vordergrund, inwiefern die angestrebte Geheimhaltung geheimdienstlicher Quellen die defensive Cyberproxy-Beziehung mit beeinflussen, im Rahmen sogenannter »Disclosure Dilemmas« (vgl. Carnegie und Carson 2020).

Wird eine öffentliche Attribution als verbale Eskalation verstanden (Steffens 2018, S. 143), könnten hierdurch auch auf der konventionellen Ebene Konflikteskalationen herbeigeführt werden. Alternativ wären die Effizienz sowie die rechtsstaatliche Integrität potenzieller Gegenmaßnahmen nur eingeschränkt gegeben, weshalb Demokratien bisher oftmals der »*tacit collusion*« (Egloff 2020b, S. 487) im Falle verdeckter Cyberoperationen den Vorzug gaben. Im Gegensatz zu ihren autokratischen Pendants erfordert der breitere Herrschaftszugang einer großen Anzahl an gesellschaftlichen Akteursgruppierungen, dass sich deren Interessen auch in der jeweiligen Außenpolitik der Demokratie widerspiegeln, um die Wiederwahl der Regierung nicht in Gefahr zu bringen. Scheitert nun aber eine demokratische Regierung bei der Beantwortung einer autokratischen Cyberaggression, etwa indem ihre Handlungen folgenlos bleiben und die Cyberangriffe ungehindert fortgeführt werden oder die demokratische Reaktion zu noch größeren Kosten für die eigene Bevölkerung führt, bestünden begründete Anreize für die Regierung, eine politische Attribution in Zukunft zu vermeiden und politischem Handlungsdruck somit aus dem Weg zu gehen. Das asymmetrische Interdependenzverhältnis besteht hierbei somit im Rahmen der Attributionsproblematik zwischen der demokratischen Regierung sowie den gesellschaftlichen Interessensgruppen mit einem Mindestmaß an Zugang zum politischen System, zumeist bereits gewährleistet durch das Wahlrecht. Ausgelöst wird die Salienz dieses Verhältnisses erst durch die offensive Cyberproxy-Nutzung autokratischer Staaten, die die asymmetrische Vulnerabilität demokratischer Regierungen auf republikanischer Ebene ausnutzen und teilweise auch offenlegen.

Der inklusivere Herrschaftszugang domestischer AkteurInnen in demokratischen Systemen, gepaart mit deren Interessen im Hinblick auf eine effiziente Beantwortung ausländischer Cyberoperationen, bedingt aus demokratischer Sicht die Konstitution des Attributionsproblems als asymmetrische Interdependenzkonstellation nach innen und außen. Trotz der beschriebenen Vorbehalte vor einer Konflikteskalation in Folge einer Attribution verlangen die Interessensdurchsetzungschancen domestischer AkteurInnen, dass auf Cyberoperationen reagiert werden *muss*, sofern diese öffentlich bekannt geworden sind. Defensive Cyberproxys können demokratischen Regierungen dabei helfen, dieses Dilemma aufzulösen, indem *sie* Attributionen vornehmen.[3] Somit wird die Informationsmanipulation durch den autokratischen Proxy-Einsatz zumindest stellvertretend in ihrer Wirkung reduziert, ohne dabei jedoch Gefahr zu laufen, unter öffentlichen Reaktionsdruck zu geraten und somit in einer Situation mit potenziell unvollständiger Information nur begrenzt rational handeln zu können. Dies könnte die Verwundbarkeit innerhalb dieser Interdependenzbeziehung sowohl gegenüber dem autokratischen Angreifer als auch gegenüber domestischen Interessensgruppen reduzieren. Der Einsatz autokratischer und demokratischer Cyberproxys im Rahmen des Attributionsinterdependenzverhältnisses ist somit bislang gegenseitig bedingt: Solange Autokratien mit ihren Cyberproxys die kritische Gewaltschwelle nicht überschreiten, verfügen Demokratien bislang auch über den notwendigen domestischen Spielraum, um ihrerseits durch den Einsatz defensiver Cyberproxys auf eine mögliche Konflikteskalation zu verzichten, frei nach dem Motto: »*Attribution is what states make of it*« (Rid

3 Dieses lässt sich auch als das Dilemma der »*Symmetrierung der Kampfstrategie vs. Asymmetrierung der Legitimität*« beschreiben (Wassermann 2014, S. 266).

und Buchanan 2015, S. 4). Dennoch liegt der Fokus der vorliegenden Arbeit in erster Linie auf dem Entstehen demokratischer und autokratischer Cyberproxy-Strategien auf Grundlage domestischer Präferenzkonstellationen. Interaktionistische Effekte im Sinne einer Tit-for-Tat-Logik können in diesem Rahmen lediglich angedeutet werden, sollten jedoch in weiteren Forschungsvorhaben expliziter im Fokus stehen, etwa im Rahmen zu identifizierender Cyberkonfliktzyklen.

3.2 Funktion und Art der Cyberproxys: Wer macht was?

Als abhängige Variable fungieren sowohl auf autokratischer als auch demokratischer Seite die beiden Aspekte der Funktion (AV I) und Art (AV II) der jeweiligen Cyberproxys. Durch diese Unterscheidung kann der Einfluss verschiedener Vulnerabilitätsasymmetrien auf ideeller, wirtschaftlicher sowie republikanischer Ebene genauer untersucht werden.

3.2.1 Funktion und Art autokratischer Cyberproxys

Es werden folgende Funktionen (AV I) autokratischer Cyberproxy-Nutzungen unterschieden, die teilweise mehrere Liberalismus-Ebenen betreffen:

Tabelle 1: Übersicht autokratischer Cyberproxy-Funktionen

Ideelle Ebene	Wirtschaftliche Ebene	Republikanische Ebene
Politische Cyberspionage	Ökonomische Cyberspionage	Überwachung Regimeeliten
Schwächung politischer Gegner (Staaten) ohne gewaltsamen konventionellen Konflikt	Militärtechnologische Cyberspionage	Überwachung Regimegegner (In- und Ausland)
Schwächung politischer Gegner (Staaten) mit gewaltsamem konventionellem Konflikt (auch durch strategisch-operative Unterstützung)	Strategisch-operative Unterstützung gewaltsamer konventioneller Konflikte	
Schwächung demokratischer Institutionen/Werte		
Überwachung Regimegegner		

(Eigene Darstellung)

1. Manipulation asymmetrischer Verwundbarkeiten auf ideeller Ebene

Cyberproxys können auf unterschiedliche Weise asymmetrische Vulnerabilitäten hinsichtlich der ideellen Ebene manipulieren:

Politische Cyberspionage vs. andere Staaten
Indem eine Autokratie demokratische Staaten auch in Friedenszeiten ausspioniert, kann sie ihre Verhandlungsmacht vergrößern. Die gewonnenen Daten können dazu beitragen, die bislang größeren demokratischen Interessensdurchsetzungschancen auf internationaler Ebene zu reduzieren und somit zunehmend die eigenen ideellen Interessen in IOs durchzusetzen. Gleiches gilt auch für bilaterale Verhandlungen zwischen besagten Staaten. Ein ähnliches Vorgehen wäre jedoch auch gegenüber rivalisierenden benachbarten Autokratien plausibel.

Schwächung politischer GegnerInnen ohne zugrunde liegendem (gewaltsamem) konventionellem Konflikt
Handelt es sich beim Gegenüber um eine militärisch überlegene Demokratie, mit der aktuell kein gewaltsamer konventioneller Konflikt besteht, können Cyberproxy-Handlungen auf die Erosion demokratischer Normen und Werte sowie das Signalisieren demokratischer Ohnmacht gegenüber den autokratischen Cyberoperationen abzielen. In beiden Fällen ist das Ziel, die ideelle Einheit des demokratischen Gegenübers zu schwächen, indem versucht wird, Einfluss auf die sozialen Identitäten der Bevölkerung zu nehmen und relative Vorteile im Rahmen dieser Interdependenzbeziehung zu erzielen. Handelt es sich beim anvisierten Staat stattdessen um eine militärisch maximal ebenbürtige Autokratie, könnten die Cyberproxy-Handlungen noch disruptivere Formen annehmen und im extremsten Falle den Cyberkonflikt in die analoge Sphäre übertragen.

Schwächung politischer GegnerInnen mit zugrunde liegendem (gewaltsamem) konventionellem Konflikt
Befindet sich eine Autokratie bereits in einem gewaltsamen konventionellen Konflikt mit einer militärisch überlegenen Demokratie, könnten ihre Cyberproxy-Handlungen darauf abzielen, diese vor allem auf moralischer Ebene zu schwächen, ohne eine Konflikteskalation zu riskieren. Die Verwundbarkeiten des demokratischen Landes im Cyberraum könnten, bei gleichzeitig konventioneller Überlegenheit, das Pflichtgefühl sowie die Verbundenheit der demokratischen Bevölkerung gegenüber der eigenen Regierung sukzessive schwächen, sofern sie keinen Ausweg aus dieser Interdependenzvulnerabilität findet. Cyberproxy-Operationen, die direkte strategische oder operative Unterstützung für diesen allgemeinen Konflikt bieten, können ebenfalls der eigenen ideellen Präferenzdurchsetzung dienen.

Schwächung/Unterminierung demokratischer Institutionen/Werte
Mithilfe von Cyberproxys können autokratische Regierungen zudem gezielt demokratische Institutionen in ideeller Hinsicht angreifen und somit untermauern, warum es auch dreißig Jahre nach Ende des Kalten Krieges zu keinem »*Ende der Geschichte*« gekommen ist (Fukuyama 2006). Gleiches gilt für zivilgesellschaftliche AkteurInnen wie Non-Governmental Organizations (NGOs) oder auch JournalistInnen und Medien-VertreterInnen, die vor allem zum Ziel von informationsgesteuerten Operationsformen werden können.

Überwachung von Regime-GegnerInnen im In- und Ausland
Zuletzt zielt auch eine Überwachung von Regime-GegnerInnen auf eine Manipulation des bestehenden ideellen Interdependenzverhältnisses ab: Gelingt es diesen, entweder zu Hause oder im Ausland gegenüber einer liberal-demokratischen Audience ihre sozialen Identitäten in Abgrenzung zu jenen des autokratischen Regimes erfolgreich zu propagieren, erhöht sich deren Herrschaftszugang zumindest indirekt. Cyberoperationen können autokratischen Regimen demnach dabei helfen, diese antizipierte Regimegefahr auf ideeller Ebene zu erkennen und zu entschärfen.[4]

2. Manipulation asymmetrischer Verwundbarkeiten auf wirtschaftlicher Ebene

Als zweite autokratische Cyberproxy-Funktion wird deren Wirken auf wirtschaftliche Interdependenzverhältnisse diskutiert:

Ökonomisch motivierte Cyberspionage
Wirtschaftsspionage kann die autokratische Abhängigkeit von ökonomisch führenden Demokratien reduzieren. Cyberproxys verringern die stärkere Vulnerabilität der meisten Autokratien auf wirtschaftlicher Ebene und schützen zugleich vor demokratischen Liberalisierungsforderungen, indem sie potenzielles ›Leapfrogging‹ ermöglichen. Somit können die wirtschaftlichen Präferenzordnungen gegenüber Demokratien trotz bestehender Inkompatibilitäten auf dieser sowie den anderen beiden Ebenen durchgesetzt werden. Gleichzeitig können domestische Output-Legitimationserfordernisse bedient werden, ohne etwas an der eigenen wirtschaftlichen Präferenzordnung ändern zu müssen (Mischung aus kommerziellem und republikanischem Argument).

Militärtechnologisch motivierte Cyberspionage
Hinsichtlich technologischer Entwicklungen argumentiert der republikanische Liberalismus, dass die demokratische Verfasstheit eines Staates im Gegensatz zum autokratischen Institutionenarrangement wirtschaftliche Innovationen grundlegend begünstigt, weil dessen Institutionen auf die legitime und inklusive Verteilung kollektiver Güter ausgerichtet sind (Moravcsik 1997, S. 531). Aufgrund der oftmals unklaren Unterscheidung zwischen ökonomisch und sicherheitspolitisch motivierter Cyberspionage wird daher auch der Diebstahl militärtechnologischer Daten als Mittel angesehen, um wirtschaftliche Abhängigkeitsverhältnisse gegenüber Demokratien auch im militärtechnologischen Bereich zu manipulieren.

Strategisch-operative Unterstützungsleistung im Rahmen eines konventionellen Konfliktes
Zuletzt besitzen auch gewaltsame konventionelle Konflikte oftmals erhebliche Implikationen für wirtschaftliche Interdependenzverhältnisse zwischen den beteiligten Staaten. Geht es beispielsweise um die Eroberung rohstoffreicher Gebiete oder für den Han-

4 Im Rahmen sog. »*Tainted Leaks*« können nach vorheriger Manipulation sensible Daten der anvisierten AkteurInnen veröffentlicht und deren Interessensdurchsetzungschancen somit geschwächt werden (Hulcoop et al. 2017).

del strategisch bedeutsamer Infrastrukturen, könnten Cyberproxys den konventionellen Streitkräften einer Autokratie in ihren militärischen Bemühungen behilflich sein. Dabei ist jedoch entsprechend dem bisherigen Forschungsstand eher von einer Substitutionswirkung auszugehen.

3. Manipulation asymmetrischer Vulnerabilitäten auf republikanischer Ebene

Cyberproxys erfüllen für autokratische Regierungen jedoch auch auf domestischer Ebene wichtige Funktionen, indem Asymmetrien im Herrschaftszugang bzw. der Interessens-durchsetzungschancen manipuliert werden können:

Überwachung/Kontrolle potenziell regimegefährdender Elitengruppierungen
Unabhängig von der Tätigkeit ist mit dem bloßen Einsatz sowie der jeweiligen institutionellen Anbindung eines Proxys eine Proxy-Funktion auf republikanischer Ebene verbunden: Durch die Beschränkung oder Erweiterung des Herrschaftszugangs bestimmter Elitengruppierungen deren Coup-Proofing-Potenzial auszubalancieren. Die republikanisch-liberalen Herrschaftserfordernisse autokratischer Systeme führen zum Gebrauch unterschiedlicher Cyberproxys. Indem kontextabhängig etwa das Militär die Kontrolle über die staatlichen APTs hat, zu anderen Zeiten jedoch der zivile Geheimdienst, kann eine autokratische Regierung entsprechend antizipierter Asymmetrien im Interdependenzverhältnis gegenüber diesen Gruppen auf republikanischer Ebene reagieren und somit einer zu starken Ermächtigung dieser Elitengruppierungen im Cyberspace vorbeugen. Gleichzeitig ermöglicht eine strengere staatliche Kontrolle der Proxys, dass auch diese ihre potenziellen Eigeninteressen nicht zu autonom im Cyberspace verfolgen können.

Überwachung von Regime-GegnerInnen im In- und Ausland
Neben den AkteurInnen der Winning Coalition stellt jedoch auch das breite Volk eine potenzielle Coup-Gefahr für autokratische Regime dar. Cyberproxys könnten dabei helfen, potenzielle Regime-GegnerInnen innerhalb der Bevölkerung im In- und Ausland zu erkennen und autokratische Informationsdefizite aufgrund des verkürzten/dysfunktionalen Transmissionsriemens auszugleichen. So soll verhindert werden, dass diese Druck auf Teile der Winning Coalition ausüben und deren Präferenzen zu Ungunsten der Regierung verändern. Mit dem Cyberproxyeinsatz wird hier das Ziel verfolgt, die Interessensdurchsetzungschancen der Regime-GegnerInnen zu verringern und die bestehende Asymmetrie auf republikanischer Ebene aus Sicht des Regimes weiterhin positiv zu gestalten.

Hinsichtlich der AV II, der Art der Proxys, steht in erster Linie die institutionelle Anbindung der in der Stellvertreterrolle agierenden AkteurInnen im Vordergrund. Zu deren Ausdifferenzierung wird auf die bestehende Forschungsliteratur zu nichtstaatlichen AngreiferInnen im Cyberspace rekurriert, die in Kapitel 1.2 vorgestellt wurde. Somit werden in erster Linie folgende Akteursgruppen als potenzielle Cyberproxy-Rollenträger konzeptualisiert:

- Cybermilizen,
- patriotische HackerInnen,
- Cyberkriminelle,
- PMSCs sowie
- nationale Forschungseinrichtungen/nationale Technologiefirmen.[5]

Die Art des Proxys kann gleichzeitig Hinweise darauf geben, wie umfassend die staatliche Verantwortlichkeit bei den jeweiligen Operationen einzuschätzen ist. Auch wenn der HD-CY.CON lediglich zwischen staatlichen, privaten und staatlich gesponserten CyberakteurInnen unterscheidet und für die oben genannte Kategorisierung die Quellen der als ›state-sponsored‹ kodierten Fälle nochmals analysiert werden müssen, soll in den Fallstudien (wenn möglich) unterschieden werden, ob bei einer Cyberproxy-Aktion der attribuierte Sponsor durch die Duldung der Proxy-Handlungen,[6] deren materielle Unterstützung oder die organisatorische Anleitung und Kontrolle in Erscheinung trat (vgl. Rivera 2015, S. 15).[7] Ein potenzieller Wandel hierbei könnte auch Aufschluss darüber geben, ob eine Autokratie ihre Proxys nach anfänglicher Distanz in Folge veränderter Attributionspraktiken demokratischer Länder nun unter zentralerer Kontrolle hält (vgl. Canfil 2020). Wichtig ist dabei im Hinblick auf die Konzeptualisierung der letztgenannten Funktionen auf republikanischer Ebene, ob sich Hinweise darauf finden lassen, welche AkteurInnen/Behörden im autokratischen System bei den jeweiligen Proxy-Operationen als staatliches Bindeglied fungierten. Dies könnte ein Indikator dafür sein, dass deren Interessensdurchsetzungschancen seitens des Regimes als potenziell ungefährlicher eingeschätzt wurden, oder aber, dass diese zum jeweiligen Zeitpunkt stärker ausgeprägt waren.

3.2.2 Funktion und Art demokratischer Cyberproxys

Für demokratische Cyberproxys wird eine weniger strikte Trennung zwischen den beiden AVs angenommen. Vielmehr ergibt sich bei diesen aus der angestrebten Funktion des Proxys auch notwendigerweise dessen Art, da das Spektrum an potenziellen AkteurInnen, die die jeweilige Handlung ausführen könnten, exklusiver ist als im Falle offensiver Cyberoperationen. Die nachfolgend aufgelisteten Funktionen werden somit priva-

5 Die bisherige Cyberproxy-Forschung behandelte diese bislang noch nicht als relevante AkteurInnen. Gerade wirtschaftlich stark nach Modernisierung strebende Autokratien könnten jedoch bei der Vorbereitung und Ausführung ihrer Cyberangriffe gezielt auf die Kenntnisse und Ressourcen nationaler Universitäten, Forschungsinstitutionen sowie staatlicher oder halbstaatlicher IT-Unternehmen zurückgreifen.

6 Für die Kategorie der Proxy-Duldung ist jedoch anzumerken, dass diese voraussichtlich am seltensten auch als Proxy-Operation attribuiert wird, aufgrund der nochmal sehr viel schwerer nachweisbaren Verletzung der ›Due Diligence‹ seitens eines autokratischen Staates. Die Ransomware-Operationen in den USA Mitte 2021 u.a. gegen die Firma Colonial Pipeline, könnten jedoch längerfristig zu einer stärkeren Adressierung dieser Sorgfaltsverantwortung seitens demokratischer Opferstaaten führen, wie es die Reaktion der US-Administration zumindest andeutete (Jasper 2021).

7 Im Abschnitt über die Operationalisierung der autokratischen AVs (Kapitel 4.4.2) wird hierzu das in der Cyberkonfliktforschung bekannte ›Spektrum staatlicher Verantwortlichkeit‹ von Jason Healey 2011 vorgestellt.

ten AkteurInnen, in erster Linie IT-Firmen, mit eigenen Threat-Research-Forschungseinheiten zugesprochen.[8] Als konstante Teilfunktion privater IT-Attributionen fungiert auf allen drei Ebenen deren Legitimationsfunktion hinsichtlich nachgelagert stattfindender politischer Attributionen.

Tabelle 2: Übersicht demokratischer Cyberproxy-Funktionen

Ideelle Ebene	Wirtschaftliche Ebene	Republikanische Ebene
Steigerung der soziopolitischen Resilienz	Steigerung der technischen Resilienz	Reduzierung des politischen Handlungsdrucks/Signaling (dauerhaft vs. temporär) bzw. Erweiterung des politischen Handlungsspielraums
Schaffung von Legitimation politischer Attributionen	Schaffung von Legitimation politischer Attributionen	Schaffung von Legitimation politischer Attributionen

(Eigene Darstellung)

1. Manipulation asymmetrischer Verwundbarkeiten auf ideeller Ebene

Stellvertretende Attributionen seitens nichtstaatlicher AkteurInnen können für demokratische Regierungen auf unterschiedliche Weise ideelle Verwundbarkeitsasymmetrien auf außenpolitischer oder domestischer Ebene manipulieren:

Reduzierung der ideellen Verwundbarkeiten gegenüber autokratischen Cyberoperationen (soziopolitische Resilienz)

Indem private AkteurInnen autokratische CyberangreiferInnen als solche benennen, lenken sie den Fokus der demokratischen Öffentlichkeit auf die Unvereinbarkeit solcher Handlungen mit den eigenen sozialen Identitäten. Somit kann zumindest teilweise der

8 An dieser Stelle könnte eingewandt werden, dass auch Medien potenziell als Attributions-Proxies fungieren könnten und dies vielleicht auch aufgrund teilweise staatlichen Interesses an dem Leaken von »*classified information*« tun (Pozen 2013). Der HD-CY.CON-Datensatz ist durch die Kategorie der ›Media-based Attribution‹ im Stande, auch dieses potenzielle Durchstechen von Infos an die Presse zu erfassen. Wenn die Quelle jedoch als ›Government Official‹ benannt wird, kann zwar von einem Durchstechen der Attribution, jedoch nicht von einer Verschleierung dieser Praxis gesprochen werden. Im Sinne der Proxy-Logik wird bei Medien zudem davon ausgegangen, dass das Veröffentlichen von Informationen der Kern ihrer Tätigkeit ist, unabhängig davon, ob dies im Interesse oder gegen den Willen der jeweiligen Regierung geschieht, was natürlich auch bei IT-Unternehmen durchaus der Fall sein kann. Jedoch wird die ›vierte Gewalt‹ wenn überhaupt, dann als institutionalisierter Proxy angesehen, da hier der oftmals typische ad-hoc-Charakter eines Proxys fehlen würde. IT-Unternehmen entwickelten erst im Laufe der Jahre eigene Attributionskapazitäten und Aktivitäten, da dies nicht von Anfang an zu ihren Tätigkeitsfeldern gehörte. Zudem gibt es auch immer noch genug Firmen, die überhaupt keine Attributionen vornehmen.

auf ideeller Ebene intendierte disruptive Effekt der Cyberhandlungen reduziert werden. Ziel dabei ist es, die Verbundenheit des demokratischen Volkes gegenüber der eigenen Regierung trotz deren potenzieller Passivität in Folge der Cyberoperation nicht schwächer werden zu lassen. Private Cyberattributionen können somit aus demokratischer Sicht die Sensitivität auf ideeller Ebene in solchen Fällen zumindest reduzieren, für den Fall, dass die demokratische Regierung keine geeigneten Maßnahmen zur Reduzierung der Vulnerabilität ergreifen kann oder will. Schafft es eine Autokratie mithilfe ihrer Cyberproxys, unterschiedliche soziale Identitäten innerhalb eines demokratischen Landes gezielt auszunutzen bzw. weiter zu polarisieren, kann diese Inkompatibilität den Handlungsspielraum demokratischer Regierungen nach innen und außen in der Folge weiter einschränken. Darüber hinaus können technische Berichte von IT-Firmen auch direkt die Resilienz demokratischer Bevölkerungen gegenüber autokratischen Cyberoperationen stärken, indem das hierfür notwendige Problembewusstsein geschaffen wird.

2. Manipulation asymmetrischer Vulnerabilitäten auf wirtschaftlicher Ebene

Die oben beschriebenen Dynamiken lassen sich ebenfalls auf autokratische Cyberoperationen mit wirtschaftlicher Zielsetzung anwenden:

Reduzierung der wirtschaftlichen Verwundbarkeiten gegenüber autokratischen Cyberoperationen (technische Resilienz)

Da etwa in liberalen Demokratien zumeist der Kapitalismus als dominantes Wirtschaftssystem Teil der sozialen Identitäten des Landes ist, lassen sich die ideelle und wirtschaftliche Ebene an dieser Stelle nicht gänzlich voneinander trennen. Indem in Folge wirtschaftlicher Cyberspionage private AkteurInnen Attributionen in Richtung autokratischer CyberangreiferInnen vornehmen, lässt sich die Cyberspionage als Angriff auf das demokratische Wirtschaftssystem und einen wichtigen Teil sozialer Identitäten darstellen. So kann der Fokus von der eigenen Verwundbarkeit auf wirtschaftlicher Ebene auf das aus ideeller Sicht zu verurteilende Handeln autokratischer Staaten verschoben werden.

Noch wichtiger ist jedoch die Präventivfunktion technischer IT-Berichte: Indem in diesen autokratische ›Techniques, Tactics and Procedures‹ (TTPs) im Cyberraum offengelegt und vor allem an wirtschaftliche AkteurInnen als Hauptadressaten vermittelt werden, kann diese stellvertretende Attribution durch ihre technische Fundiertheit bestehende Vulnerabilitäten einer Demokratie reduzieren.

3. Manipulation asymmetrischer Verwundbarkeiten auf republikanischer Ebene

Auch defensive Cyberproxys können für demokratische Regierungen gegenüber der domestischen Audience eine bedeutende Funktion auf republikanischer Ebene erfüllen:

Manipulation asymmetrischer Verwundbarkeiten auf republikanischer Ebene (Reduzierung politischen Handlungsdrucks/Signaling)

Demokratische Regierungen können defensive Cyberproxys nutzen, um ihre im Ver-

gleich zu Autokratien stärkere Vulnerabilität gegenüber einer Vielzahl an domestischen AkteurInnen auf republikanischer Ebene zu manipulieren.[9] Dies kann auch das Ausbalancieren der Interdependenzen der Regierung mit der eigenen Geheimdienstcommunity, der politischen Opposition oder KritikerInnen der eigenen Partei bedeuten. Geheimdienste sind oftmals Vetospieler öffentlicher Attributionen, da sie fürchten, hierdurch einen Teil ihrer Attributionsvektoren durch deren Offenlegung zu ›verlieren‹. Die Opposition oder andere, nicht in der Regierung vertretene AkteurInnen des politischen Systems sowie der Bevölkerung, haben gleichzeitig jedoch oftmals ein Interesse an öffentlicher Attribution. Somit können defensive Cyberproxys das aufgezeigte Handlungsdilemma für demokratische Regierungen zumindest reduzieren. Indem der Proxy eine öffentliche Attribution vornimmt, kann dem Angreifer sowie der Öffentlichkeit signalisiert werden, dass der Täter bekannt ist. Gleichzeitig gerät die Regierung selbst jedoch nicht unter ähnlichen Handlungsdruck wie im Falle einer eigenen Attribution und muss keine Attributionskapazitäten der Geheimdienste offenlegen.[10]

Hinsichtlich der AV II, der Art der demokratischen Cyberproxys, wird in dieser Arbeit argumentiert, dass eine Lücke zwischen primär technischer sowie politischer Attribution existiert, weshalb Firmen aus dem IT-Bereich bzw. potenziell auch frei arbeitende IT-ExpertInnen mit entsprechenden technischen Fähigkeiten als relevante Proxys konzeptualisiert werden müssen. Eine weitere Spezifizierung dabei lautet, dass hauptsächlich nationale IT-Firmen, die in dieser Rolle für ein demokratisches Land agieren, als Proxys konzeptualisiert werden.[11] Aufgrund des besonderen Delegationsmodus dieser Proxy-Nutzungen könnte bei fehlenden nationalen Ressourcen nicht einfach wie im Falle von ›Hacking-for-Hire‹-Prozessen auf ausländische AkteurInnen ausgewichen werden. Dass demokratische Regierungen ausländischen IT-Firmen oder Internet-Service-Providern (ISPs) Geld oder Aussicht auf Regierungsaufträge für die jeweilige Proxy-Funktionserfüllung anbieten könnten, erscheint weniger plausibel als eine Fokussierung auf nationale AkteurInnen, sofern diese vorhanden sind. Ein Grund hierfür ist der öffentliche Charakter der Attribution als Proxy-Funktion. Der Stellvertreter kann nicht, wie bei offensiven Cyberoperationen, verdeckt operieren, da in diesem Handlungsfeld nicht die Handlung oder Urheberschaft, sondern die staatliche Verantwortlichkeit verschleiert werden soll.[12] Reichweite, Legitimität und Wirkung stellvertretender Attributionen

---

9 Interview mit einem leitenden Mitarbeiter eines deutschen Bundesministeriums, am 02.12.2020.

10 Inwiefern eine solche Verschleierungstaktik politischer Verantwortlichkeiten jedoch im Rahmen unterschiedlicher Kontexte als wahrscheinlicher gelten kann als in anderen, wird Gegenstand der Konzeptualisierungen der übrigen Variablen sein. Zudem könnte eine stellvertretende Attribution lediglich zeitlich begrenzt das Attributionsvakuum demokratischer Regierungen füllen, sowie nachgelagerten politischen Attribution mithilfe technischer Evidenzen die notwendige Legitimität verleihen.

11 Selbstverständlich können auch ausländische, international agierende Firmen eine stellvertretende Attribution vornehmen. Jedoch lässt sich bei diesen der Delegationscharakter schwerer plausibilisieren, als im Falle nationaler Unternehmen, die ideelle, ökonomische, rechtliche und manchmal sogar politische sowie personelle Interdependenzen zu ihren jeweiligen Regierungen aufweisen.

12 Anders formuliert will die demokratische Regierung verschleiern, dass ihre Informationslage eine eigene Attribution sehr wohl zulassen würde, die es jedoch aufgrund möglicher Fehlschlüsse,

dürften bei nationalen IT-Firmen weitaus größer eingestuft werden als bei ausländischen VertreterInnen. Ein weiterer wichtiger Grund besteht in den immateriellen und materiellen Anreizstrukturen, die seitens einer Regierung für Firmen innerhalb der nationalen Rechtsprechung ausgeprägter sein dürften als für ausländische Unternehmen.

3.3 Gesellschaftliche Präferenzkonstellationen als unabhängige Variable

Entsprechend der liberalen Theorieverortung stellen die jeweiligen gesellschaftlichen Präferenzen innerhalb autokratischer und demokratischer Staaten sowie deren Kompatibilität zueinander die Haupterklärungsvariable staatlicher Cyberproxy-Strategien dar. Aufgrund der daraus resultierenden Verwundbarkeitsasymmetrien entscheiden diese darüber, ob und wie beide Regimetypen die genannten Proxy-Funktionen bedienen wollen.

3.3.1 Autokratien

Unabhängig von den notwendigen technischen Voraussetzungen bedarf es konfliktiver Präferenzkonstellationen auf ideeller, wirtschaftlicher oder republikanischer Ebene zwischen einer Autokratie und anderen Staaten, damit Cyberoperationen im Allgemeinen und deren Durchführung mithilfe von Proxys im Besonderen für die Autokratie von Interesse sind. Dies ist der Fall, sobald Proxys entweder die eigenen Verwundbarkeiten innerhalb dieser Interdependenz verringern oder die Verwundbarkeiten des Gegenübers verstärken/ausnutzen sollen. In beiden Fällen ist die Wirkung eigener oder fremder Verwundbarkeitsasymmetrien zentral. Die erste Hypothese lautet daher:

> *H1: Je größer die eigene Verwundbarkeit im Rahmen konfliktiver Präferenzinkompatibilitäten zu anderen Staaten auf einer oder allen drei Liberalismus-Ebenen ist, desto größer sind die autokratischen Anreize für die Nutzung offensiver Cyberproxys.*

Grundlegend besitzen Autokratien auch untereinander konfliktive Präferenzkonstellationen. Verantwortlich hierfür können gegenseitig kostenverursachende domestische Präferenzen auf ideeller oder wirtschaftlicher Ebene sein, die vor allem auch zwischen unterschiedlichen Subtypen stärker ausgeprägt sein können. Zugleich könnte der dominante Herrschaftszugang einer bestimmten Elitengruppierung in einem autokratischen Subtyp die Interessensdurchsetzungschancen eines anderen einschränken, wodurch auch auf republikanischer Ebene intra-autokratische Varianzen zum Tragen kommen können. Der autokratische Subregimetyp kann somit als Teil des Ausdrucks der domestischen Präferenzkonstellation angesehen werden, der sich in erster Linie auf republikanischer Ebene niederschlägt. Daher beeinflusst er als Bestandteil der UV implizit mit, in welchem Ausmaß die beschriebenen Präferenzkonstellationen auf ideeller und kommerzieller Ebene erst entstehen können.

geheim zu haltender Geheimdienstmethoden, sowie oftmals fehlender Reaktionsoptionen zu verhindern gilt.

Prinzipiell können Präferenzinkompatibilitäten, die zugleich mit asymmetrisch verteilten Kosten im Rahmen einer wahrgenommenen Interdependenzbeziehung einhergehen, jedoch häufiger zwischen Autokratien und Demokratien vermutet werden, da zwischen den beiden Hauptregimetypen auf allen drei Liberalismus-Ebenen die größten grundlegenden Unterschiede bestehen. Die zweite Hypothese in Bezug auf autokratische Cyberproxy-Strategien lautet somit:

H2: Je stärker aufgrund konfliktiver Präferenzkonstellationen Regimetypenunterschiede in asymmetrischen Verwundbarkeiten resultieren, desto stärker sind die autokratischen Anreize für eine offensive Cyberproxy-Nutzung dem jeweiligen Staat gegenüber.

Der dritte Zusammenhang zwischen UV und AVs verweist nochmals auf die Ausdifferenzierung letzterer: So resultieren die inhaltliche Funktion eines offensiven Cyberproxys, die Form und das Zielprofil der von ihm ausgeführten Cyberoperationen direkt aus der Ausgestaltung der hierfür maßgeblichen Verwundbarkeitsasymmetrie, basierend auf der Präferenzkonstellation zwischen den Staaten. Zwei Beispiele verdeutlichen diese Annahme: Eine Autokratie kann sowohl gegenüber anderen Autokratien als auch gegenüber Demokratien inkompatible Präferenzkonstellationen auf ideeller Ebene aufweisen. In beiden Szenarien ist für die Auswahl der jeweiligen Cyberoperationsform entscheidend, durch welche die angestrebte Manipulation der bestehenden Verwundbarkeitsasymmetrie am ehesten erreicht werden kann. Grundlegend erscheinen informationsbasierte Operationsformen wie Hack-and-Leak-Operationen hierfür geeigneter als verdeckt angelegte Cyberspionage-Operationen. Dieselbe Logik kann auf Präferenzinkompatibilitäten zwischen Autokratien und anderen Staaten auf wirtschaftlicher Ebene angewendet werden: Hierbei können Cyberspionage-Operationen mit dem Ziel, die wirtschaftlichen Informationsasymmetrien im Technologie-Bereich zum eigenen Vorteil zu manipulieren, als prinzipiell vorteilhafter eingestuft werden als etwa disruptive Cyberoperationen auf kritische Infrastrukturen.[13] Diese exemplarischen Ausführungen resultieren in folgender, dritter Hypothese:

H3: Je größer der erwartete Nutzen bestimmter Formen offensiver Cyberproxy-Operationen zur Reduzierung eigener Verwundbarkeiten auf ideeller und/oder wirtschaftlicher Ebene ist, desto wahrscheinlicher ist deren Anwendung seitens der jeweiligen Autokratie.

Zuletzt werden hinsichtlich des Wirkens der republikanischen Ebene auf die Art und institutionelle Anbindung autokratischer Cyberproxys (AV II) die innerautokratischen Präferenzkonstellationen betrachtet. Diesen wird ein direkter Einfluss darauf unterstellt, welche AkteurInnen eine autokratische Regierung als offensive Proxys in Betracht zieht und durch welche Elitengruppierungen deren Kontrolle/Leitung erfolgt:

13 Inkompatibilitäten zwischen Autokratien und Demokratien auf wirtschaftlicher Ebene können zudem Ausdruck oder auch Auslöser gleichzeitiger Interessenskonflikte auf ideeller Ebene sein. Wie bereits erwähnt, beziehen sich die sozialen Identitäten domestischer Akteursgruppen auch auf die jeweiligen Vorstellungen legitimer Verteilung öffentlicher Güter, mit somit direkten Implikationen für den wirtschaftlichen Bereich.

H4: Je größer die domestischen Verwundbarkeiten autokratischer Regierungen auf republikanischer Ebene aufgrund inkompatibler Präferenzkonstellationen sind, desto eher sind die Auswahl und institutionelle Anbindung der Proxys auch auf deren Manipulation ausgerichtet.

Gegenüber der eigenen Winning Coalition könnte dies bedeuten, dass ein autokratisches Regime die Kontrolle über seine Cyberproxys gezielt einer gewissen Akteursgruppe *nicht* anvertraut, sofern diese zum Regime inkompatible Präferenzen aufweist und somit im Cyberspace nicht noch stärker ermächtigt werden soll. Da jedoch neben Putschversuchen der Winning Coalition auch von unten entstehende Protestbewegungen breiterer Teile der Bevölkerung einem autokratischen Regime trotz Repressionsmaßnahmen gefährlich werden können, könnte dies eine engere Kontrolle nichtstaatlicher Cyberproxys oder die Instrumentalisierung im Ausland stationierter HackerInnen zur Folge haben.

3.3.2 Demokratien

Auf demokratischer Seite werden ebenfalls verschiedene Präferenzkonstellationen auf ideeller, wirtschaftlicher sowie republikanischer Ebene als Haupterklärungsvariable für die beschriebene defensive Cyberproxy-Nutzung konzeptualisiert. Sofern dabei vonseiten autokratischer Staaten die eigenen Verwundbarkeitsasymmetrien durch offensive Cyberoperationen regelmäßig ausgenutzt werden, sollten auch entsprechende Anreize für eine defensive Cyberproxy-Nutzung vorliegen. Das Konfliktpotenzial der domestischen Präferenzkonstellation im Verhältnis zu vor allem autokratischen Staaten beeinflusst somit wie auch im Falle der Autokratien die demokratische Cyberproxy-Nutzung:

H1: Je umfassender die eigenen Verwundbarkeiten im Rahmen konfliktiver Präferenzinkompatibilitäten zu anderen Staaten auf einer oder allen drei Liberalismus-Ebenen durch offensive Cyberoperationen ausgenutzt werden, desto größer sind die demokratischen Anreize für die Nutzung defensiver Cyberproxys.

Auch für demokratische Staaten gilt, dass diese sehr wohl auch untereinander konfliktive Präferenzkonstellationen auf einer oder mehreren der drei Liberalismus-Ebenen aufweisen können. So zeichnen sich liberale und illiberale Demokratien zwar durch die Gemeinsamkeit weitgehend freier und fairer Wahlen auf republikanischer Ebene aus, jedoch entwickeln sich letztere in den letzten Jahren zunehmend in Richtung elektoraler Autokratien, indem der Wahlprozess und dessen Integrität durch verschiedene AkteurInnen unterminiert werden (Levitsky und Ziblatt 2018). Hierfür werden vor allem Veränderungen der Präferenzkonstellationen auf der ideellen Ebene verantwortlich gemacht, die zwischen liberalen und illiberalen Demokratien potenziell auch zu steigenden Konfliktpotenzialen auf außenpolitischer Ebene führen können. Auch der demokratische Subtyp kann somit als Teil des Ausdrucks der domestischen Präferenzkonstellation angesehen werden und beeinflusst als Bestandteil der UV implizit mit, in welchem Ausmaß die beschriebenen Präferenzinkompatibilitäten auf ideeller, kommerzieller oder republikanischer Ebene erst entstehen können.

Nichtsdestotrotz wird auch bei Demokratien davon ausgegangen, dass die Verwundbarkeitsasymmetrie zwischen den beiden Regimetypenlagern größere Ausmaße annehmen dürfte als zwischen Demokratien untereinander, insbesondere im Cyberspace. So-

mit bestehen prinzipiell für Autokratien mehr Anreize und Möglichkeiten, Verwundbarkeiten demokratischer Länder im Cyberspace häufiger auszunutzen, da sie aufgrund der hier existierenden Asymmetrie regelmäßig im Vorteil sind.

Da, wie erwähnt, für demokratische Cyberproxys im Rahmen dieser Arbeit hinsichtlich der Art des Proxys eine geringere Varianz konzeptualisiert wird, bezieht sich die zweite Hypothese auf den Zusammenhang zwischen UV und AV I. Zwar wird grundlegend der stellvertretende Attributionsakt als defensive Funktion demokratischer Cyberproxys definiert, jedoch zeigte die Konzeptualisierung der AV I auch hier hinsichtlich über die bloße Verantwortungszuschreibung hinausgehender Funktionen technischer IT-Berichte eine gewisse Subvarianz auf. So können mit diesen technische Resilienzfunktionen bezüglich des Schließens von Sicherheitslücken oder einer allgemeinen Steigerung des Gefahrenbewusstseins besonders bedrohter Akteursgruppen verbunden sein. Als zweite Subfunktion wurde die Legitimation einer potenziell nachgelagerten, politischen Attribution benannt, die zum gleichen Attributionsschluss wie der technische Bericht kommt, hierfür jedoch aufgrund vorliegender Geheimhaltungserwägungen nicht die entsprechenden Evidenzen liefern kann. Welcher erweiterte Zweck mit einer gänzlich oder zeitlich begrenzten stellvertretenden Attribution für eine demokratische Regierung einhergehen kann, ist somit ebenfalls davon abhängig, inwiefern hierdurch die durch den Cyberangriff ausgenutzten bzw. offengelegten Verwundbarkeiten reduziert werden können.

> *H2: Je größer der erwartete Nutzen bestimmter Formen defensiver Cyberproxy-Operationen (Attributionen) zur Reduzierung eigener Verwundbarkeiten auf ideeller, wirtschaftlicher sowie republikanischer Ebene, desto wahrscheinlicher ist deren Anwendung seitens der jeweiligen Demokratie.*

Ein Beispiel soll die hierbei angenommene Logik verdeutlichen: Erscheint es im Falle einer autokratischen Cyberoperation aus Sicht einer demokratischen Regierung ausreichend, die eigenen, technischen Verwundbarkeiten im Sinne einer Offenlegung der TTPs des Angreifers seitens eines defensiven Proxys zu stärken, ist eine nachgelagerte politische Reaktion unwahrscheinlicher. Wenn jedoch aufgrund des Profils und der Wirkweise der Operation bzw. aufgrund des Profils des Angreifers auch eine direkte, politische Signalwirkung ermöglicht werden soll, könnte die technische Attribution einer später erfolgenden politischen Attribution mehr Glaubwürdigkeit verleihen, vorausgesetzt, ihre Erkenntnisse deuten in dieselbe Richtung. Dasselbe gilt auch, falls der politische Handlungsdruck trotz erfolgter technischer Attribution so hoch ist, dass zu einem gewissen Zeitpunkt auch eine politische Attribution erfolgen *muss*.

3.4 Die nationale Cyberakteursumwelt als konditionierende Variable

Als konditionierende Variable wird in dieser Arbeit die nationale Cyberakteursumwelt konzeptualisiert. Dieser Begriff bedarf genauerer Spezifizierung: Unabhängig von der inhaltlichen Ausgestaltung der domestischen Präferenzordnungen bedingen die Existenz und Diversität staatlicher sowie nichtstaatlicher AkteurInnen, die im oder den Cyberspace betreffend aktiv sind, in welchem Umfang Autokratien oder Demokratien zur

Manipulation antizipierter Interdependenzverhältnisse auf offensive oder defensive Cyberproxys zugreifen können, wenn sie es wollen. Hierfür werden AkteurInnen auf vier Ebenen unterschieden: der staatlich-behördlichen, der privatwirtschaftlichen, der zivilgesellschaftlichen sowie der kriminellen Ebene.

3.4.1 Autokratien

Die zur Verfügung stehende Auswahl der Mittel im offensiven Cyberbereich wird entscheidend durch die jeweiligen Entwicklungen eines Landes im Sektor der Information and Communication Technology (ICT) beeinflusst. Diese wird definiert als die »*actual technology-based systems on which information is commonly stored and/or transmitted*« (Solms & van Niekerk 2013: 98). Während hierzu zu Beginn nur die Telekommunikation zählte, werden in diesem Konzept heute die immer stärker verschmelzenden Bereiche des Fernsehens, der Telefonie sowie des Internets, die zumeist durch einen einzigen ISP zu den EndnutzerInnen transportiert werden, zusammengefasst. Auf staatlich-behördlicher Ebene ist somit entscheidend, ob eine Autokratie bereits zu Beginn oder im Laufe des Untersuchungszeitraumes staatliche Einheiten in militärischen und/oder zivilen Behörden mit eigenen Fähigkeiten zur Durchführung offensiver Maßnahmen im Cyberspace etablierte. Ist dies der Fall und wurde dennoch eine offensive Cyberproxy-Nutzung bescheinigt, deutet dies aufgrund prinzipiell eigener technischer Fähigkeiten bereits auf eine geringere Erklärungskraft des staatlichen Motivs der technischen Ermächtigung durch Proxys hin. Möglich wäre jedoch eine anfängliche Unterstützung noch im Aufbau befindlicher Cybereinheiten durch Proxys, die schrittweise in diese integriert oder aber durch deren Handlungen obsolet werden könnten.

Auf privatwirtschaftlicher Ebene wird für die Bewertung der KV das Vorhandensein technologisch versierter IT-Unternehmen mit jeweilig autokratischer Herkunft analysiert. Wie bereits angedeutet wurde, können auch IT-Unternehmen für autokratische Regierungen offensive Cyberoperationen durchführen. Somit wird für die KV ein komprimiertes Lagebild privatwirtschaftlicher Technologieunternehmen mit mutmaßlich offensiven Cyberkapazitäten der jeweiligen Autokratie erstellt, um den prinzipiellen Proxy-Pool auf dieser Ebene bewerten zu können.

Auch der zivilgesellschaftliche Sektor kann Cyberproxys hervorbringen: Hierunter werden vor allem sog. HacktivistInnen, patriotische HackerInnen, aber auch Studierende/AbsolventInnen informationstechnologischer Studiengänge der autokratischen Fallbeispiele verstanden. Verfügt ein Land zu Beginn oder im Laufe des Untersuchungszeitraums über entsprechende AkteurInnen, so könnten diese bei Bedarf auch als Proxys eingesetzt werden.[14]

Zuletzt konstituiert der nationale Cyberkriminalitätssektor den dritten Proxy-Pool autokratischer Regime. So wird davon ausgegangen, dass Autokratien mit florierender Cyberkriminalität bei Bedarf auch entsprechend auf diese zurückgreifen werden, um Cyberoperationen zu ermöglichen. Entscheidend wird hierbei jedoch im Rahmen der

14 So könnten in heimischen Universitäten, oder aber im Ausland ausgebildete Informatikstudierende, als AgentInnen rekrutiert, oder aber in weniger institutionalisierten ad hoc-Beziehungen temporär als Proxys genutzt werden (Bronk und Tikk-Ringas 2013, S. 8).

Analyse der AV II sein, wie sich das Staat-Proxy-Verhältnis im jeweiligen Fall charakterisieren lässt, ob durch finanzielle Anreize, patriotische Gesinnung oder aber physischen/rechtlichen Zwang. Theoretisch formuliert beeinflusst die KV somit auf autokratischer Seite, ob die aufgrund konfliktiver Präferenzinkompatibilitäten wahrgenommenen Verwundbarkeitsasymmetrien mithilfe offensiver Cyberproxys überhaupt zum eigenen Vorteil gestaltet werden *könnten*. Die Cyberproxy-Nutzung durch Autokratien mit ausreichenden staatlichen Fähigkeiten und Ressourcen im ICT-Bereich betont zudem die beschriebenen politischen Funktionen der nichtstaatlichen StellvertreterInnen auf republikanischer Ebene nach innen und außen.

Hinsichtlich der (zumindest zu Beginn des Untersuchungszeitraums) vorliegenden Dominanz militärischer oder ziviler AkteurInnen im offensiven Cyberbereich könnte hierbei zudem von Belang sein, welche der beiden Seiten in der historischen Entwicklung der staatlichen ICT-Kapazitäten bzw. bei der Etablierung staatlicher Cyberfähigkeiten die Oberhand hatte. Dies könnte erklären, welche AkteurInnen den anfänglichen Cyberkonfliktaustrag und somit auch die Proxy-Nutzung aufgrund ihres auch im Cyberspace stärker ausgeprägten Herrschaftszugangs zum jeweiligen Zeitpunkt hauptsächlich bestimmten.

3.4.2 Demokratien

Um die primär defensive Cyberproxy-Nutzung demokratischer Staaten erklären zu können, kommt der KV ein noch größerer Stellenwert zu als im Falle der Autokratien. Analog sagt sie jedoch nicht notwendigerweise etwas darüber aus, ob eine Demokratie tatsächlich auf defensive Cyberproxys zurückgreift. Auf Seiten der Demokratien entscheidet sich jedoch bereits bei der jeweiligen Ausprägung der KV, ob nationale IT-Firmen stellvertretende Attribution überhaupt durchführen könnten und ob deren Berichte auch die notwendige Aufmerksamkeit erfahren würden.[15] Wie bei der Konzeptualisierung der AV aufgezeigt, wird im Falle demokratischer Proxys von einer primären Fokussierung auf nationale AkteurInnen ausgegangen, da für ausländische Proxys der für Demokratien von vornherein als schwächer anzunehmende Delegationsmechanismus im Falle defizitärer Ressourcen kaum mehr glaubwürdig plausibilisiert werden kann. Somit gilt es auch im Falle demokratischer Cyberproxy-Nutzung im Rahmen der empirischen Analyse zu untersuchen, inwiefern die privatwirtschaftlichen Potenziale im Cyber-Threat-Research-Bereich des Landes einen Einfluss hierauf hatten. Verfügt eine Demokratie in nicht ausreichendem Maße über technisch sophistizierte, mit hinreichender internationaler Reputation und Reichweite ausgestattete IT-Firmen, sind ihre Möglichkeiten zur defensiven Cyberproxy-Nutzung von vornherein eingeschränkt, auch wenn die Ausprägung der UV für einen solchen Gebrauch spricht.

15 Im Rahmen der »*weaponization of interdependencies*« von Farrell and Newman 2019 würde dies deren sog. »*panopticon*«-Effekt entsprechen: Bei diesem können Staaten zur »*weaponization*« ihrer privilegierten Stellung in globalen Netzwerken die hierbei an den Knotenpunkten gesammelten Informationen gezielt zum eigenen Vorteil verwenden, so wie auch Demokratien mit entsprechenden ICT-Niveaus die Daten/Erfahrungen ihrer nationalen IT-Firmen mit Zugang zu globalen Kundendaten zur Manipulation asymmetrischer Interdependenzbeziehungen einsetzen können.

3.5 Der Einfluss konventioneller Konfliktdynamiken als intervenierende Variable

Als intervenierende Variable (IV) fungiert das allgemeine Konfliktniveau bzw. dessen Dynamiken im Hinblick auf dessen Eingreifen in die Beziehung zwischen UV und AVs. Wie bei der Konzeptualisierung von AVs und UVs teilweise bereits angedeutet wurde, können Konfliktgeschehnisse der analogen Welt sowohl auf autokratische als auch demokratische Cyberproxy-Strategien erheblichen Einfluss nehmen.

3.5.1 Autokratien

Der Nutzen offensiver Cyberoperationen, entweder zur Vermeidung gewaltsamer konventioneller Konflikte oder zur erfolgreichen Gestaltung derselbigen, wurde in der Forschung unterschiedlich beurteilt. Besonders in Folge von Stuxnet wurde dem Internet eine geradezu potenziell pazifizierende Wirkung attestiert: Speziell Sabotage und Spionage wurden dabei im Rahmen eines »*Cool War*« im Cyberspace als mögliche Game-Changer im staatlichen Konfliktaustrag benannt (Arquilla 2012; Rid 2013). Entgegen der ebenfalls weit verbreiteten Eskalationsbefürchtungen ermögliche die diskutierte Offense-Dominance im Cyberspace somit gerade eine friedlichere, analoge Sphäre und unter der Bedingung der bis dato noch nicht erfolgten menschlichen Verluste in Folge eines Cyberangriffs. Im Sinne des »*ex-ante bargaining*« nach Fearon (1995, S. 380) seien Cybertools eine Option, um drohende offene und gewaltsame Konflikte doch noch abwenden zu können (Brantly 2014, S. 465). Durch sie können laut Brantly die Aspekte der »*information asymmetries, issue indivisibilities, and commitment problem*« und somit auch die Wahrscheinlichkeit eines offenen Krieges vermindert werden (2014, S. 472).[16]

In Folge der immer deutlicher werdenden Zurückhaltung von Staaten gegenüber Stuxnet ähnelnden regelmäßigen Cyberoperationen wurde dieses zielgerichtete ›Coercion‹-Potenzial von Cyberangriffen jedoch immer stärker angezweifelt. Stattdessen seien Cybertools überwiegend als Komplementärstrategien im Rahmen traditioneller Konfliktaustragungspfade zu verstehen, da sie nur in Kombination mit diesen eine ›coercive‹ Wirkung entfalten würden (Borghard und Lonergan 2017; Valeriano et al. 2018, S. 3). Cyberoperationen wird somit immer stärker das Potenzial zur Herbeiführung einer Verhaltensänderung bei einem gegnerischen Akteur abgesprochen, insbesondere bei einem bereits in Gang gesetzten konventionellen Konflikt (Kostyuk und Zhukov 2019). Aus diesem Grund wird in dieser Arbeit *nicht* argumentiert, dass der Einsatz von Cyberproxys auf militärischer Ebene eher zu Erfolgen oder Misserfolgen führen würde. Stattdessen soll durch die Konzeptualisierung der IV gezeigt werden, dass in Friedens- und Kriegszeiten unterschiedliche Anreize zu varianten Proxy-Nutzungen seitens unterschiedlicher autokratischer AkteurInnen wirken.

Für auf der konventionellen Ebene noch nicht militärisch eskalierte Konflikte sollten autokratische Cyberproxys eine stärkere Rolle zur Eskalationskontrolle zwischen der

16 Auch die Forschung zu Eskalationsdynamiken im Cyberspace deutet darauf hin, dass Cyberoperationen (zumindest in westlichen Demokratien wie den USA) eher als deeskalierendes Konfliktaustragungsmittel gesehen werden (Kreps und Schneider 2019).

konventionellen und Cyber-Konfliktebene spielen, insbesondere gegenüber konventionell militärisch überlegenen Demokratien. Befindet sich eine Autokratie jedoch bereits in einer militärischen Auseinandersetzung mit einem militärisch überlegenen Staat (potenziell begründet durch eine Allianzsituation), sollten Cyberproxys stärker der Manipulation der Verwundbarkeitsasymmetrie dienen, indem durch deren disruptiven Einsatz die größere Verwundbarkeit des Gegenübers im Cyberraum noch stärker ausgenutzt wird als in Friedenszeiten. Somit lautet die erste Hypothese hinsichtlich des Wirkens der IV:

> *H1: Je gewaltsamer das bestehende allgemeine Konfliktniveau ist, desto wahrscheinlicher ist auch ein intensiverer/disruptiverer Einsatz autokratischer Cyberproxys, etwa gegen kritische Infrastrukturen des Gegners.*

Aus Sicht der Plausible Deniability erscheint jedoch der Einsatz von Proxys bei bestehenden staatlichen Cyberfähigkeiten in einer solchen Situation weniger notwendig zu sein, da der Konflikt ja bereits gewaltsam eskaliert ist. Der offensive Einsatz autokratischer Cyberproxys in gewaltsamen konventionellen Konflikten könnte somit auf defizitäre staatliche Cyberkapazitäten hinweisen. Andererseits könnte dies darauf hindeuten, dass das Regime trotz eigener staatlicher Cyberfähigkeiten im Rahmen republikanischer Interdependenzbeziehungen gegenüber domestischen AkteurInnen wie dem Militär Proxys bevorzugt.

Hinzu kommt aus republikanischer Sicht, dass autokratische Regime bei der Entscheidung, ob sie einen Konflikt gewaltsam eskalieren lassen, weniger domestischen Restriktionen unterworfen sind als demokratische Regierungen. Wenn offensive Cyberangriffe zur Unterstützung militärischer Angriffe auf dem analogen Schlachtfeld dienen sollen, könnte es aus autokratischer Sicht sinnvoll erscheinen, beide Bereiche in ›eine Hand‹ und damit wahrscheinlicher in die des Militärs zu geben, da dieses in Kriegszeiten gegenüber zivilen Geheimdiensten meist einen verstärkten Herrschaftszugang innehat. Drei Aspekte tragen zu dieser erhöhten »*Organizational Salience*« des Militärs in Kriegszeiten bei (Legro 1996, S. 122):

1. Dessen Monopol über die Kriegsdomäne;
2. Die Komplexität der Kriegsdomäne, nochmals verstärkt durch das Hinzukommen des Cyberspace als ›Fifth Domain‹;
3. Der zeitlich begrenzte Entscheidungs- und Handlungskorridor.

Zudem ist der offensive Gebrauch von Cyberkonfliktmitteln im Sinne von Sabotage oder Disruption auch völkerrechtlich leichter in militärischer als in ziviler Verantwortung zu rechtfertigen (Boeke und Broeders 2018, S. 78). Somit lautet die zweite Hypothese im Hinblick auf das Wirken der IV:

> *H2: Je stärker die angewandten Cyberoperationen Verwundbarkeitsasymmetrien im Rahmen militärischer Konflikte manipulieren sollen, desto eher ist von einer militärischen Kontrolle autokratischer Cyberproxys auszugehen.*

Zusammenfassend kann somit konstatiert werden, dass für Autokratien, die sich bereits in gewaltsamen konventionellen Konflikten befinden, von einem intensiveren Ein-

satz der stärker militärisch geführten Cyberproxys auszugehen ist. Gleiches gilt für sich intensivierende, bislang gewaltfreie Konflikte, jedoch ohne die notwendigerweise verstärkte militärische Proxy-Anleitung. Dagegen ist in friedlicheren Zeiten nicht nur die Verschleierung der eigenen Urheberschaft, sondern auch der Tat an sich öfter das Ziel.

3.5.2 Demokratien

Auch für die Proxy-Nutzung demokratischer Staaten wird deren allgemeine Konfliktinvolvierung als IV konzeptualisiert. Grundlegend bedingen die aufgezeigten Inkompatibilitäten zu den Präferenzordnungen vor allem autokratischer Staaten mit größerer Wahrscheinlichkeit eine stärkere demokratische Involvierung in gewaltsame konventionelle Konflikte. Demokratische Regierungen führen aus unterschiedlichen Motivlagen mit überwiegend autokratischen Kontrahenten Krieg. Politische, militärische und ideelle Beweggründe bilden die hierbei mögliche Spannbreite ab.[17] Steht die autokratische Interessensdurchsetzung auf außenpolitischer Ebene den Interessen demokratischer Regierungen gleich auf allen drei Ebenen im Weg, müsste dies dem liberalen Argument nach wahrscheinlicher zu konventionellen Konflikten zwischen den Parteien führen. Damit wird nicht behauptet, dass Krieg in jedem Falle das unumgängliche Resultat einer solchen Konstellation sei, lediglich wird eine größere Wahrscheinlichkeit dieses Outcomes plausibilisiert.

Für die Attribution als defensive Cyberproxy-Tätigkeit bedeutet dies, dass die Involvierung demokratischer Staaten in konventionelle Konflikte deren Attraktivität für Cyberangriffe aus autokratischer Sicht verstärken kann. Obgleich auch in Friedenszeiten von Cyberoperationen autokratischer KontrahentInnen ausgegangen wird, könnten deren Häufigkeit und Intensität im Kontext gewaltsamer Auseinandersetzungen zunehmen (komplementär zur H1 der IV bei Autokratien). Als Konsequenz könnte der Handlungsdruck auf die Regierung in Folge von Cyberangriffen auf kritische Infrastrukturen oder zivile Ziele steigen.[18] Somit lautet für demokratische Staaten die erste Hypothese zum Wirken der IV:

> *H1: Je stärker die asymmetrische Verwundbarkeit demokratischer Staaten im Cyberraum im Rahmen gewaltsamer konventioneller Konflikte seitens Autokratien manipuliert/ausgenutzt wird, desto wahrscheinlicher ist eine demokratische Cyberproxy-Nutzung.*

Eine alternative Schlussfolgerung wäre jedoch, dass demokratische Regierungen, die sich bereits in einem gewaltsamen konventionellen Konflikt mit einer oder mehreren Autokratien befinden, auch weniger davor zurückschrecken sollten, selbst Cyberangriffe zu attribuieren, da die allgemeine Eskalation des Konfliktes ja bereits erfolgt ist. Sollte dies regelmäßig der Fall sein, so wäre jedoch nach wie vor die Frage, welche Formen

---

17 Wenn die eigenen ideellen Werte anscheinend (oder auch nur scheinbar) in Gefahr sind und das Wahlvolk aufgrund historischer Pfadabhängigkeit ein positiveres Verhältnis zum eigenen Interventionismus hat, kann dieses Vorgehen bei ausreichender Erfolgsaussicht sogar seitens der BürgerInnen mitgetragen werden (Lacquement 2004, S. 43).

18 Gleiches gilt für kommerzielle Ziele im Falle der beschriebenen Handelskonflikte mit einem entsprechend hohen Intensitätsniveau.

die jeweilige Verantwortungszuweisung politischer EntscheidungsträgerInnen dabei annimmt und welchen Einfluss der demokratische Subtypus hat, gerade im Hinblick auf damit verbundene politische Reaktionen.[19] Diese Überlegungen werden in folgende Hypothese überführt:

H2: Je stärker eine demokratische Regierung bereits auf der konventionellen Ebene Sanktionsmöglichkeiten gegenüber einem autokratischen Cyberangreifer in Stellung gebracht oder angewandt hat, desto wahrscheinlicher ist eine lediglich substituierende Proxy-Attribution.

3.6 Staaten und ihre Proxys: Die Suche nach dem perfekten Match

Der vorgestellte liberale Erklärungsansatz regimetypenspezifischer Cyberproxy-Strategien beruht in erster Linie auf der komplexen Wirkweise unterschiedlicher domestischer Präferenzkonstellationen mit varianten Verwundbarkeitsasymmetrien auf den drei Liberalismus-Ebenen als Folge. Diese asymmetrischen Vulnerabilitäten zum eigenen Vorteil zu manipulieren, wird dabei als der übergeordnete Zweck autokratischer und demokratischer Cyberproxy-Aktivitäten angesehen. Das grundlegend inverse Verhältnis zwischen der eigenen Verwundbarkeit nach innen und außen begründet dabei die für Autokratien offensive Nutzung vs. der defensiveren Instrumentalisierung seitens demokratischer Regierungen. Aufgrund der unterschiedlichen Verwundbarkeiten auf der konventionellen und Cyber-Ebene nutzen Autokratien regelmäßiger letztere, um ihre Unterlegenheit im analogen Bereich auszugleichen. Dabei visieren sie insbesondere demokratische Informationsasymmetrien auf republikanischer Ebene an, was wiederum den Bedarf an demokratischer Proxy-Nutzung zur Folge hat, um diese Verwundbarkeitsasymmetrie zum eigenen Vorteil zu manipulieren.

Kein Gegenstand der vorliegenden Arbeit, jedoch für die Zukunft von Interesse könnte sein, inwiefern Demokratien versuchen sollten, auf analogem Wege die zugunsten autokratischer Regime ausgestalteten Informationsasymmetrien gegenüber deren Bevölkerungen aufzuweichen, ohne ihnen Vorwände für weitere Repressionsmaßnahmen zu liefern.

Grundlegend wird für beide Regimetypen die jeweilige Cyberproxy-Strategie als prävalent angesehen. Dennoch zeigt die Konzeptualisierung der KV und IV, dass davon unabhängig länder- sowie kontextspezifische Faktoren ebenfalls einen Einfluss auf den Zusammenhang zwischen UV und AVs nehmen können, sodass eben nicht davon auszugehen ist, dass alle Autokratien und alle Demokratien Cyberproxys gleichermaßen nutzen. Inwiefern jedoch zumindest für die vier Untersuchungsfälle deren Cyberproxys das ›perfekte Match‹ für das jeweils angestrebte Eskalationsmanagement darstellen, muss die empirische Analyse zeigen. Zuvor werden jedoch das Untersuchungsdesign sowie die dabei angewandte Methodik vorgestellt.

19 Falls die Demokratie jedoch trotz bereits erfolgter Kampfhandlungen weitere Eskalationen auf der konventionellen Ebene verhindern wollen sollte, könnte dies dennoch für die vermutete Cyberproxy-Nutzung sprechen. In ihrer 2021 veröffentlichten Dissertation beschäftigte sich bereits Heajune Lee mit dem Einfluss der Eskalationsrichtung einer Konfliktdyade auf das öffentliche Cyberattributionsverhalten der USA.

4. Das Mixed-Methods-Forschungsdesign

Das vorliegende Forschungsdesign folgt einem zweistufigen Aufbau. Der HD-CY.CON-Cyberkonfliktdatensatz bildet die Grundlage für den ersten quantitativen Analyseschritt. Hierbei werden die Daten im Sinne der deskriptiven Statistik aufbereitet und ausgewertet. Die daraus entstehenden Grafiken und Schaubilder eröffnen den Blick auf die vorherrschende staatliche Proxy-Nutzung und legen somit die Grundlage für die anschließende Fallauswahl. In einem zweiten Schritt erfolgt die eigentliche Analyse im Rahmen des strukturiert-fokussierten Vergleichs, um durch die qualitative Untersuchung der quantitativ ausgewählten Fälle die notwendige Analysetiefe zu erhalten. Das Untersuchungsdesign gehört somit zur Kategorie der Mixed Methods (Kelle 2014, S. 153).

Im Folgenden wird die empirische Datenbasis der Arbeit genauer vorgestellt: Der HD-CY.CON ist ein Cyberkonfliktdatensatz, der seit 2016 an der Universität Heidelberg im Rahmen mehrerer Forschungsprojekte entstanden ist und fortgeführt werden soll.[1] Die Autorin war seit 2017 an der Konzeptualisierung und Kodiertätigkeit des Datensatzes beteiligt (ab 2019 hauptverantwortlich), weshalb ein entsprechender Zugang sowie die notwendigen Kenntnisse im Umgang mit dem Datensatz bestehen.

Zunächst werden jedoch Erschwernisse sowie bestehende Forschungsprojekte im adressierten Forschungsfeld identifiziert und diskutiert.

4.1 Methodische Herausforderungen im Bereich der Cyberkonfliktforschung

»*Active representation of the threat landscape is the goal, but the reality is that the picture of the cyber security threat landscape we currently have is incomplete, misleading, or outright fake*« (Valeriano und Maness 2018, S. 50). Zu dieser Einschätzung gelangten Brandon Valeriano und Ryan C. Maness nicht etwa zu Beginn des sog. ›Cyber-Hypes‹, der sich in Folge des

1 Von 2016–2017 und 2017–2018 im Rahmen zweier Förderlinien der Exzellenzinitiative der Universität Heidelberg (Field of Focus-4), sowie grundlegend von 2019–2021 seitens der Deutschen Stiftung Friedensforschung innerhalb des Projektes »Sicherheit durch Verschleierung: Warum Regierungen Proxies in Cyberkonflikten einsetzen«.

ersten ›Cyber-Wars‹ in Estland 2007, der Cyberangriffe auf Georgien 2008 sowie des Bekanntwerdens von Stuxnet 2010 entwickelte, sondern im Jahr 2018. Das Attributionsproblem, ungleich verteilte Ressourcen zu dessen Lösung sowie Geheimhaltungserwägungen im Zusammenhang mit Cyberoperationen auf Angreifer- und Opfer-Seite wurden dabei bislang seitens der Forschung als zentrale Widrigkeiten hinsichtlich quantitativer Vorhaben im Bereich der Cyberkonfliktforschung angeführt (Hansel und Nanni 2018, S. 215; Griffith 2018; Healey 2018). In ihrer Arbeit aus 2018 befassten sich Valeriano und Maness mit den Grenzen und Möglichkeiten der Quantifizierung von Cyberkonflikten. Darin plädieren sie dafür, dass trotz der unstrittigen Herausforderungen in *jedem* Forschungsfeld einmal ein Anfang gemacht werden muss(te). Somit sollten quantitative Cyberkonfliktprojekte vermehrt angegangen, dabei jedoch stets hinsichtlich potenzieller Verzerrungen oder theoretischer Einschränkungen reflektiert werden. Dies sei eine Grundherausforderung, besonders auch für informierte Entscheidungen politischer EntscheidungsträgerInnen, die sich mit Cyberkonflikten konfrontiert sehen.

An den Grundsatz »*Reality is a Social Construction*« (Valeriano und Maness 2018, S. 51) knüpft auch der HD-CY.CON an, der nicht etwa den Anspruch postuliert, sämtliche vorgefallene Cyberoperationen zwischen staatlichen und/oder nichtstaatlichen AkteurInnen erfassen zu können, sondern durch die Beleuchtung der öffentlich sichtbaren Angriffe sowie des politischen Umgangs damit wichtige Dynamiken des Forschungsgegenstandes offenzulegen.[2]

Valeriano und Maness arbeiteten zum Zeitpunkt des oben genannten Zitates bereits an der zweiten Version ihres ›Dyadic Cyber Incident and Dispute Datasets‹ (DCID), dessen erste Fassung rein staatliche Cyberattacken zwischen bereits bekannten Rivalen für die Jahre 2001 bis 2011 umfasste (insgesamt 110 Vorfälle; Valeriano und Maness 2014, S. 356). Der DCID stellte in einer bis dato auf qualitative Fallstudien konzentrierten Forschungslandschaft den ersten Versuch dar, die nur schwer zugängliche Cyberkonfliktlandschaft auch quantitativ zu vermessen. Somit konnten die Autoren in der Folge zwei ihrer zentralen theoretischen Thesen durch ihre empirischen Daten stützen: Zum einen die bereits beschriebene These der staatlichen Zurückhaltung (restraint) im Cyberspace, die das relativ niedrige Konfliktniveau im Cyberspace trotz weitreichender technischer Möglichkeiten aus verschiedenen Perspektiven zu erklären vermag (Valeriano und Maness 2014; Valeriano und Maness 2015; Borghard und Lonergan 2019). Zum anderen indizierten ihre gesammelten Cyberkonfliktdaten eine fast nicht nachweisbare Beziehung zwischen der konventionellen und Cyber-Konfliktebene im Sinne eines potenziellen Spill-Overs (Maness und Valeriano 2016a), was in der Folge von weiteren Autoren bestätigt wurde (Kostyuk und Zhukov 2019).

Somit wurde erstmals eine Alternative zum bis dato vorherrschenden methodischen Vorgehen offeriert, das über den Vergleich weniger Cyberoperationen (desselben Cyberangreifers) zumeist nicht hinausreichte (u.a. Hjortdal 2011; Axelrod und Iliev 2014; Blank

2 Die Metapher eines Eisberges, bei dem stets nur der Teil oberhalb des Wasserspiegels sichtbar ist, wird für das Deepweb verwendet (Bergman 2001) und greift auch für Cyberoperationen: Auch wenn ein signifikanter Teil von Attacken stets im Verborgenen bleiben wird, so können über die umfassende Analyse des sichtbaren Teils dennoch wichtige Erkenntnisse über deren Wirkweise und Auswirkungen gewonnen werden.

2017; Ji-Young et al. 2019). Nichtsdestotrotz konnte bislang auch der DCID aufgrund seines inhaltlichen Zuschnitts auf rein staatliche Konflikttätigkeit, zudem zwischen bereits in der analogen Welt rivalisierten Staaten, sowie weiterer Einschränkungen für viele theoretische Fragen keine adäquate empirische Grundlage bilden. Zu nennen wäre die wenig bis kaum ausdifferenzierte Kodierung der Kategorie des attribuierten Angreifers, wobei nicht zwischen direktstaatlichen sowie staatlich gelenkten/unterstützten Proxy-Angriffen unterschieden wird.[3]

Des Weiteren erlaubt der DCID keine Aussagen über die jeweilige Quelle der Attribution, d.h., wer die Verantwortungszuweisung im jeweiligen Fall vorgenommen hat. Auch werden nicht nur Cyberoperationen mit tatsächlich öffentlich bekannter Verletzung der CIA-Triade vom DCID inkludiert, sondern auch lediglich ›versuchte‹ Cyberoperationen.[4] Kritisch zu betrachten ist auch die in Version 1.5 eingeführte ›Interaction-Type‹-Kategorie: Hierbei erfolgt implizit eine Interpretation der Motivlage des Cyberangreifers, nämlich hinsichtlich der Frage, ob es sich um eine Defensiv- oder Offensivoperation gehandelt hat (Maness et al. 2019, S. 5). Den Anfang einer Cyberkonfliktinteraktion auszumachen, ist aufgrund potenziell nicht öffentlich gemachter Angriffe schwierig, weshalb auch eine Klassifizierung einer scheinbar lediglich auf Verteidigung ausgerichteten Cyberoperation zumindest hinterfragt werden muss.[5] Des Weiteren erschwert der bereits herausgestellte Unterschied zwischen lediglich auf allgemeine Spionage ausgerichteten Infiltrationen fremder Netzwerke und der als Vorstufe einer potenziell folgenden Manipulation des Zielsystems dienenden Infiltration eine solche Bewertung.

Einen weiteren Forschungsansatz im Bereich der stärker quantitativ basierten Cyberkonfliktforschung stellt die ›Cyber-Event-Liste‹ des Center for Strategic and International Studies (CSIS) dar, eine rein beschreibende Auflistung von Cyberoperationen ohne systematische Kriterien der Attribution, der Angriffs-Kategorisierung oder der Intensität (CSIS 2020). Im Gegensatz hierzu fokussiert sich der ›Cyber Operations Tracker‹ des Council on Foreign Relations (CFR) auf »*state-sponsored cyberattacks*« (CFR 2020). Somit ignoriert dieser jedoch Cyberoperationen vonseiten nichtstaatlicher AkteurInnen, die

---

3 Im Rahmen der Veröffentlichung der Version 1.5 des DCID, im Juni 2019, kündigten die Autoren an, in der künftigen Version 2.0 erstmals auch nichtstaatliche AkteurInnen sowie alle möglichen Staaten-Dyaden erfassen zu wollen. Version 1.5 legte einen größeren Fokus auf den jeweiligen Kontext der Cyberoperationen und führte neue Variablen ein, wie die Kategorie der »*cyber-enabled information-operations*« (Maness et al. 2019, S. 2). Zum Zeitpunkt der Einreichung dieser Arbeit stand Version 2.0 jedoch noch nicht der Öffentlichkeit zur Verfügung.

4 So wird der Zweck einer Kategorie der Version 1.5 wie folgt beschrieben: »*Whether or not the incident successfully achieved its objective; did it breach the target's network and fulfill its intended purpose*« (Maness et al. 2019, S. 4). Für eine derartige Bewertung bedarf es jedoch einer plausiblen Einschätzung dieses »*objective*« des jeweiligen Angreifers, was aufgrund des beschriebenen Cybersicherheitsdilemmas oft erschwert wird.

5 Die Unterscheidung, ob eine Operation defensiver oder offensiver Natur ist, hängt zudem von dem Wissen über potenziell zuvor erfolgte Operationen innerhalb der betreffenden Konfliktdyade ab. Darüber hinaus können sprachliche Darstellungen der Operationen erheblichen Einfluss auf eine solche Interpretation nehmen und sich nicht mit der Interpretation des jeweiligen Opfers decken, der die Operation womöglich nicht als defensiv empfunden hat. Bemerkenswert ist zudem, dass einer der beiden Urheber des DCID, Brandon Valeriano, ansonsten gegen die Anwendung der ›Offense vs. Defense‹-Unterscheidung im Cyberspace plädiert (Valeriano 2021).

ebenfalls politische Wirkung entfalten können. Die Beurteilung, dass der jeweilige Fall als staatlich gesponsert zu bewerten ist, geht zudem nicht in jedem der erfassten Angriffe aus den verlinkten Quellen hervor (z.B. für die Gruppierung ›Hellsing‹), was jedoch in einzelnen Fällen auch auf den DCID zutrifft, z.B. für dessen Südkorea-Attribution des sog. ›Earthquake-Hacks‹ aus 2011. Zudem wird (ebenfalls bei beiden Projekten) über eine mögliche Anfechtung der Attribution durch andere AkteurInnen keine Auskunft gegeben. Ebenso fehlt (beim CFR-Tracker) eine Kategorie zur Bewertung der jeweiligen Intensität bzw. Schwere des Vorfalls.

Gemein ist allen drei genannten Ansätzen (DCID; CSIS; CFR), dass sich diese ausschließlich auf englischsprachige Quellen beziehen. Somit könnte eine potenzielle Verzerrung im Sinne regionaler bzw. sprachlich-kultureller Blindflecken bei der Aufnahme relevanter Cyberoperationen die Folge sein (Sparks 2003). Zudem würde die Inklusion nicht englischsprachiger Quellen die Möglichkeit bieten, potenziell existierende konkurrierende Attributionen zu bestimmten Fällen zu ermitteln und somit politisch motivierte Verantwortungszuweisungen als solche zu entlarven (Zetter 2017b).

4.2 Der HD-CY.CON-Datensatz

Aufbauend auf der Konfliktdefinition des Heidelberger Instituts für Internationale Konfliktforschung (HIIK) werden Cyberkonflikte im Rahmen des HD-CY.CON als eine »*Interesseninkompatibilität zwischen mindestens zwei AkteurInnen im Hinblick auf einen bestimmten Konfliktgegenstand*« (HIIK 2016, S. 6), ausgetragen durch Cyberoperationen, definiert. Orientiert am Kernverständnis von IT-Sicherheit, werden in der Arbeit hierunter Handlungen zusammengefasst, die einen oder mehrere Bereiche der sog. CIA-Triade der Informationssicherheit verletzen (Confidentiality; Integrity; Availability; Andress 2014, S. 5). Diese interaktionistische Konfliktdefinition und das differenzierte Kodierverfahren (siehe Abschnitt 4.2.1) ermöglichen eine detailliertere Betrachtung der politischen Dimension des Konfliktaustrags, etwa der Salienz erfasster Cyberkonfliktgegenstände (Steiger et al. 2018, S. 84). Demokratien werden entsprechend des ›Freedom in the World Index‹ von Freedom House anhand des Labels »*free*« im entsprechenden Operationsstartjahr definiert, gleiches gilt für autokratische Staaten hinsichtlich der Kategorisierung »*not free*« (Freedom House 2019).

4.2.1 Theoretische Annahmen und Implikationen

Zunächst gilt es zu klären, welche Arten von Cyberoperationen für den HD-CY.CON relevant sind und auf Grundlage welcher Kriterien deren Bewertung erfolgt. Wie Valeriano und Maness richtig konstatieren, bedeutet die Festlegung dieser Inklusionskriterien einen entscheidenden Schritt im Prozess der Entwicklung jedes Konfliktdatensatzes (Valeriano und Maness 2018, S. 57). Der HD-CY.CON wendet hierbei drei grundlegende Kriterien an (Harnisch et al. 2021, S. 1):

1. Deutet die Attribution auf einen staatlichen Angreifer, einen staatlich unterstützten Angreifer (Proxy) oder einen nichtstaatlichen Akteur mit offensichtlich politischer Motivation (z.B. das Hackerkollektiv Anonymous) hin?[6]
2. Ist ein politisches Ziel oder sind mehrere politische Ziele unter den Opfern, z.B. Politiker, Ministerien, staatliche Verwaltungsbehörden oder militärische bzw. polizeiliche Einrichtungen?[7]
3. Wurde die Cyberoperation im Sinne einer verbalen Adressierung des Vorfalles durch PolitikerInnen politisiert?[8]

Trifft eines (oder treffen mehrere) dieser Inklusionskriterien zu, wird der recherchierte Angriff in den Datensatz aufgenommen und anhand des Codebooks kodiert. Wichtig ist zudem, dass informationsbasierte Beeinflussungsoperationen wie Fake News, die nicht die CIA-Triade der Informationssicherheit verletzen, entsprechend dem technisch dominierten Verständnis von Cybersicherheit kein Gegenstand des Datensatzes sind (Schünemann 2020, S. 202). Des Weiteren muss ein erkennbarer Schaden aus den erfassten Quellen hervorgehen, lediglich versuchte Operationen fallen somit ebenfalls aus dem Datensatz heraus (Steiger et al. 2018, S. 90).

Die drei Inklusionskriterien veranschaulichen die möglichst große Spannbreite an Cyberoperationen mit potenziell politischer Dimension, die seitens des HD-CY.CON abgedeckt werden. Dabei erfüllt er zudem Forderungen aus der Forschung an künftige Vorhaben, z.B. die differenzierte Inklusion nichtstaatlicher AkteurInnen sowie von Cyberoperationen im Rahmen innerstaatlicher Repression (Valeriano und Maness 2018, S. 57).

Im Folgenden werden zentrale theoretische Aspekte des HD-CY.CON und seines zugrunde liegenden Codebooks vorgestellt und diskutiert.

4.2.1.1 Attribution

Die Bedeutung der Attribution von Cyberoperationen reicht immer stärker über die rein technische Ebene hinaus und wird zunehmend zum Politikum. Der HD-CY.CON trägt diesem Umstand in besonderer Weise Rechnung: Durch eine multiperspektivische Kodierung von Attributionen wird die Offenlegung unterschiedlicher Attributionslogiken möglich. Auch wenn an dieser Stelle die bereits dargelegte technische Komplexität der Attribution von Cyberangriffen keinesfalls als trivial abgetan werden soll (vgl. Rid und Buchanan 2015; Berghel 2017), lassen sich durch dieses Vorgehen dennoch die unterschiedlichen Attributionsmaßstäbe der verschiedenen AkteurInnen erfassen. Für jeden im Datensatz kodierten Fall wurden möglichst sämtliche potenziell getätigten Verantwortungszuweisungen recherchiert: des Opfers selbst, der Regierung des jeweiligen Opfers (falls es sich dabei z.B. um eine Firma gehandelt hat), des Täters,[9] der IT-Sicherheits-

6 AkteurInnen wie Anonymous oder andere, nichtstaatliche CyberangreiferInnen mit politischer Motivation werden als ›Hacktivists‹ bezeichnet.

7 Eine detaillierte Auflistung der politischen Ziel-Kategorien findet sich im frei zugänglichen Codebook des HD-CY.CON.

8 Bestreitet ein beschuldigter Staat lediglich die Schuld an einer Cyberoperation, so wird dieser Sprechakt im Rahmen des HD-CY.CON noch nicht als Politisierung bewertet.

9 Eine solche Selbstzuschreibung ist jedoch bislang überwiegend bei HacktivistInnen wie Anonymous vorzufinden, oder auch nichtstaatlichen, patriotischen Hackergruppierungen, deren zu-

branche sowie anderer DrittakteurInnen wie Forschungsinstituten oder Geheimdiensten befreundeter Staaten (Steiger et al. 2018: 84).[10] Jede Attribution wird dabei in zwei Kategorien unterteilt: das attribuierte Land des oder der Täter(s) sowie die Kategorisierung des Akteurs/der AkteurInnen.[11] Dabei muss nicht für beide Kategorien in jedem Fall eine Attribution vorliegen. So werden Cyberoperationen oftmals lediglich einem geografischen Ursprung zugeordnet, ohne jedoch weitere Aussagen über die genauen TäterInnen zu treffen, und umgekehrt. Wichtig ist hierbei, dass, anders als beim Cyber Operations Tracker des CFR, eine gewisse Eindeutigkeit bei der Attribution gewährleistet sein muss.[12] Äußert etwa eine IT-Firma, dass eine seriöse Attributionsbewertung nicht möglich ist, auch wenn einige Spuren in eine Richtung deuten, so wird die Initiator-Category (=Angreifer-Kategorie) seitens der IT-Sicherheitsbranche für diesen Fall mit ›0‹ und damit als ›unknown‹ kodiert.

Die Inklusion der Attributionen des Privatsektors in Form eigenständiger Cyber-Threat-Research-Berichte bzw. umfassender Analysen zu bestimmten Angriffen kann dabei helfen, rein politisch motivierte Attributionen als solche zu entlarven und im Sinne der technischen Evidenzen in Frage zu stellen (Steiger et al. 2018, S. 84). Unterstützt wird dieses Ansinnen durch die Kodierung der jeweiligen Länder, aus denen die attribuierenden IT-Firmen stammen, um potenzielle Verbindungen zu politischen Attributionstaktiken verschiedener Regierungen aufzeigen zu können.[13] Somit ist eine Vermessung des

meist ideologisch motiviertes Ziel es ist, dass das anvisierte Opfer (und bestenfalls die ganze Welt) von ihren Taten und Fähigkeiten erfährt. Eine Analyse zu dieser »*voluntary attribution*« erstellten (Poznansky and Perkoski 2018). Dabei identifizierten sie unterschiedliche Motivlagen für freiwillige Selbstattribution zwischen Staaten und nichtstaatlichen AkteurInnen. Erstere ließen sich hierauf vor allen Dingen dann ein, wenn der jeweilige Gegner im Sinne von coercion durch die Cyberoperation zu etwas gezwungen werden sollte, während nichtstaatliche HackerInnen hierdurch wie erwähnt in erster Linie ihre Fähigkeiten zur Schau stellen wollen (Poznansky und Perkoski 2018, S. 402). Auch Floyd untersuchte in einer Arbeit aus 2018, in welchen Fällen eine »*self-attribution*« und somit die Aufgabe des konstatierten »*attribution-advantage*« aus staatlicher Sicht Sinn ergibt. Jedoch lassen sich bislang eher selten freiwillige Verantwortungseingeständnisse von staatlicher Seite finden, ein Beispiel hierfür wären jedoch die selbst proklamierten (jedoch durch wenig operative Details unterfütterten) Cyberangriffe der USA sowie Großbritanniens auf Ziele des sog. Islamischen Staates (Seals 2018; Temple-Raston 2019).

10 Bekanntestes Beispiel für einen solchen Fall ist bis dato die Informationsweitergabe des niederländischen Geheimdienstes AIVD (Algemene Inlichtingen- en Veiligheidsdienst) an die US-Behörden im Vorfeld der Wahlmanipulation 2016. Der AIVD hatte Zugriff auf die Computer einer der involvierten russischen Hackergruppierungen, Cozy Bear und konnte somit deren Agieren gegen das DNC live mitverfolgen, die US-Behörden alarmieren sowie die im Nachgang erfolgte US-Attribution in Richtung des Kremls stützen, auch wenn dies vonseiten der Niederlande nicht öffentlich geschah (Noack 2018).

11 Auf staatlicher Seite sieht das Codebook folgende Initiator-Kategorien vor: ›State‹ (1), ›Non-state-actor‹, ›state-sponsorship suggested‹ (Proxy) (2) sowie ›Non-state-actor, state-sponsorship suggested, widely held view, but not invoked in this case‹ (2,1) (für Akteure, die im Allgemeinen als staatliche Proxies angesehen, im betreffenden Fall von der Attributionsquelle jedoch nicht konkret als solche benannt werden).

12 Wie bereits erwähnt, lassen sich manche Attributionseinordnungen des CFR Tracker anhand der angegebenen Quellen nicht nachvollziehen.

13 Die entsprechende Kategorie lautet ›Country of Origin: IT-Attribution‹ und befand sich noch nicht in dem von Steiger et al. 2018 vorgestellten Codebook.

vermuteten Graubereiches zwischen erfolgter technischer und nach wie vor oftmals unterlassener politischer Attribution möglich.

Die Gegenüberstellung politischer und stärker technisch basierter Attributionen der IT-Firmen ermöglicht zudem, potenzielle Widersprüchlichkeiten bestimmter Verantwortungs-zuweisungen aufzudecken (Steiger et al. 2018, S. 84). So kann es beispielsweise dazu kommen, dass Attributionen politischer AkteurInnen im Nachhinein nach erfolgten technischen Analysen seitens der IT-Sicherheitsbranche angezweifelt oder widerlegt werden. Der Grad der ›Contestation‹ von Cyberattributionen wird auch in der Forschung zunehmend untersucht (z.B. Egloff 2020a) und im HD-CY.CON auf Grundlage der Kategorie ›Attribution-Basis‹ wiedergegeben. Diese gibt an, von welchem Akteur die jeweils kodierte Attribution stammt. Bei potenziell mehreren attribuierenden AkteurInnen kann es hier auch zu mehrfachen Kodierungen kommen.[14] Finden sich widersprüchliche Attributionen verschiedener AkteurInnen, wird im Rahmen der Attribution-Basis-Kategorie zusätzlich zu den Codes der jeweiligen UrheberInnen der Verantwortungszuweisung der Code ›4‹ kodiert, der für eine ›Contested Attribution‹ steht. Die Beurteilung, welche Zuweisung plausibler ist, übersteigt jedoch den Anspruch des Datensatzes.

Da öffentliche Verantwortungszuweisungen oft erst nach einer gewissen Zeit erfolgen, kodiert der HD-CY.CON (wie auch der DCID) Cyberoperationen für einen bestimmten Zeitraum frühestens mit einem Jahr Abstand (Steiger et al. 2018, S. 81). Auch werden die getätigten Attributions-Kodierungen immer wieder notwendigerweise aktualisiert, da Attributionen im Cyberspace oftmals nicht als final angesehen werden können. Ein Beispiel wären False-Flag-Attacken (auch ›Fourth-Party-Collection‹ genannt; vgl. Guerrero-Saade und Raiu 2017), wie sie etwa im Falle der jahrelang seitens der russischen APT Turla gekaperten und für eigene Angriffe genutzten IT-Infrastruktur der iranischen APT OilRig 2019 bekannt wurden (Corera 2019).

4.2.1.2 Intensität

Die traditionelle Konfliktforschung sah lange Zeit die Mortalitätsrate eines Konfliktes als das entscheidende Kriterium dafür an, wie intensiv dieser zu bewerten sei und ob dabei bereits von einem Krieg gesprochen werden kann. Die prominentesten Beispiele hierfür sind der Correlates of War-Index (COW) sowie das Uppsala Conflict Data Program (UCDP). In der Folge kam es jedoch auch zu alternativen Ansätzen der Klassifizierung und Bewertung unterschiedlicher Konflikte: Das Konfliktbarometer des Heidelber-

14 Durch die zusätzliche Kodierung der Form der Attribution kann zudem ein regelmäßiges ›Durchstechen‹ von Attributionen mithilfe der Vierten Gewalt als mögliches Handlungsmuster vor allem in demokratischen Staaten aufgedeckt werden. Direkte, öffentlich getätigte Attributionen von staatlicher Seite wären dagegen: Erklärungen der Regierung, technische Berichte/Warnungen (alerts), öffentlich getätigte geheimdienstliche Bewertungen sowie strafrechtliche Anklageerhebungen oder Sanktionen (Romanosky und Boudreaux 2021). Hinzu kommt, dass auch Attributionen seitens zivilgesellschaftlicher Akteure, wie NGOs oder Forschungseinrichtungen erfasst werden (›Attribution by Third Party‹). Somit soll dem bereits identifizierten Bias zu Gunsten der Aufarbeitung von Cyberoperationen gegen kommerzielle AkteurInnen durch private IT-Firmen Rechnung getragen und hierdurch auch relevante Angriffe auf die Zivilgesellschaft umfassender abgebildet werden können (Maschmeyer et al. 2020).

ger Instituts für internationale Konfliktforschung bewertet Konflikte nicht nur anhand der Anzahl menschlicher Opfer, sondern auch durch die Betrachtung von verschiedenen Konfliktmaßnahmen, Konfliktereignissen und vor allem Konfliktgegenständen. Somit wird der Fokus nicht ausschließlich auf die gewaltsamste Form von Konflikten gelegt. Stattdessen wird im Rahmen eines Stufenmodells die Analyse potenzieller Transformationen in eskalativer oder deeskalativer Richtung ermöglicht (HIIK 2016).

Der DCID sieht im Gegensatz zu den eher deskriptiven CFR und CSIS eine eigene Intensitätsskala vor. Deren Zustandekommen bzw. die dieser zugrunde liegenden Bewertungskriterien konnten dabei jedoch nicht gänzlich transparent und konsistent sichtbar gemacht werden: So kann die beispielhafte Aufzählung einzelner Fälle zu den jeweiligen Kategorien keine alleinige und ausreichende Anleitung für Dritte liefern, die das Schema auf andere Fälle zu übertragen versuchen. Es bleibt somit unklar, wie konkret beispielsweise »*Type 4*«, also Incidents mit einem »*dramatic effect on a country*«, von »*Type 5*«, also Vorfällen mit einem »*escalated dramatic effect on a country*«, zu unterscheiden wären (Valeriano und Maness 2014, S. 353). Trotz dieser Defizite hinsichtlich der Übertragbarkeit der Intensitätsmessung liefert das Vorgehen des DCID wichtige und auch für den HD-CY.CON relevante Anhaltspunkte für das eigene Vorgehen: So sieht auch dieser die Möglichkeit vor, dass Cyberangriffe eine besonders schwerwiegende Auswirkung auf grundlegende Kernfunktionen einer betroffenen Gesellschaft haben können. Der sog. ›Target-Multiplier‹ beinhaltet eine Multiplikation des zuvor errechneten ungewichteten Intensitätswertes mit 1,5, für den Fall, dass der jeweilige Cyberangriff eine gesamtgesellschaftlich als besonders kritisch anzusehende Wirkung entfaltet hat. Dies trifft zu, wenn durch den Cyberangriff Teile der kritischen Infrastrukturen[15] so getroffen werden, dass daraus nicht nur partielle, sondern zumindest regionale Folgen erwachsen (beispielsweise flächendeckende Stromausfälle in einem Land oder die Beeinträchtigung der Wasserversorgung signifikanter Teile der Bevölkerung etc.), oder, wenn die nationalen Angriffs- oder Verteidigungskapazitäten und -fähigkeiten eines Landes durch den Angriff zumindest zwischenzeitlich erheblich gestört werden (bspw. durch das Paralysieren militärisch bedeutsamer Satelliten oder die Störung der Flugsysteme von Kampfjets etc.) (Steiger et al. 2018, S. 87). Im Wissen, dass diese Kriterien keinesfalls als ›hart‹ gelten und somit nicht durch konkrete Grenzwerte erfasst werden können, ergänzt dieser Multiplikator die eigentliche Intensitätsbemessung lediglich. Der ungewichtete Cyberintensitätswert entsteht vielmehr durch die Aufsummierung aller Werte in den verschiedenen technischen Kategorien des HD-CY.CON, die folgende Aspekte beinhalten: Art des Angriffes (Incident-Type) sowie potenzielle physische Schäden (räumlich und zeitlich). Aufgrund der nicht existierenden direkten Zuweisung menschlicher Todesopfer als Folge von Cyberangriffen (Lonsdale 2019) wird die ›Casualties‹-Kategorie bislang noch als eine ergän-

15 Die Definition der kritischen Infrastrukturen im Rahmen des HD-CY.CON erfolgte auf Grundlage der Selektion eines von möglichst vielen Staaten geteilten Verständnisses der hierunter zu fassenden Teilbereiche. Auch wenn z.B. die USA in Folge der Wahlen 2016 ihre Wahlsysteme ebenfalls als kritisch einstuften, traf dies bislang jedoch noch nicht auf das Gros der anderen Staaten zu. Falls sich dies in den kommenden Jahren ändern sollte, müsste die Kategorie entsprechend angepasst werden.

zende Zusatzkategorie geführt.[16] Physische Effekte werden erfasst, da untersucht werden soll, inwiefern die steigenden Potenziale für Cyberangriffe mit Auswirkungen ähnlich physischer Gewalt auch tatsächlich ausgenutzt werden. Gerade disruptive Angriffe auf kritische Infrastrukturen[17] werden am ehesten als gerechtfertigte Szenarien für den Begriff ›Cyberwar‹ genannt, was somit durch diese Kategorie gesondert erfasst werden kann (Nye 2011).

Der HD-CY.CON unterscheidet zwischen folgenden Angriffsarten: ›Data Theft‹ (mit oder ohne Doxing), ›Disruption‹, ›Hijacking‹ (mit oder ohne Missbrauch). Bei diesen Kategorien wird davon ausgegangen, dass sie am umfassendsten in der Lage sind, alle möglichen Varianten digitaler Angriffsstrukturen bzw. deren Auswirkungen abzubilden. Aufgrund der beschriebenen Schwierigkeit, Intentionen von CyberangreiferInnen zweifelsfrei festzustellen, ist die Erfassung der tatsächlichen Folgen unter Berücksichtigung von Kontextfaktoren, die zumindest partiell Aufschluss darüber geben können, ob es sich dabei um intendierte oder unintendierte Auswirkungen handelt, die gebotene Herangehensweise.[18] Unter Data Theft wird jede Form der vom Opfer unautorisierten Exfiltration von Daten des Zielsystems verstanden.[19] Das häufigste Einfallstor für CyberangreiferInnen stellen dabei nach wie vor technisch eher wenig sophistizierte Phishing-Kampagnen oder auch Social-Engineering-Methoden dar.[20] Jedoch kommen auch Watering-Hole-, oder Living-off-the-Land-Methoden häufig zum Einsatz (Bisson

16 In einer Studie von Choi et al. 2019 stellten die Autoren fest, dass in Krankenhäusern, die in Folgen von »*data breaches*« mit der Wiederherstellung der betroffenen Systeme zu kämpfen hatten, die Mortalitätsrate unter bestimmten Patienten in der direkten Folge anstieg, im Vergleich zum Zeitraum davor. Diese »*data breaches*« wurden in der Studie jedoch nicht ausschließlich durch Hacking-Angriffe wie Ransomware-Attacken herbeigeführt, sondern auch etwa durch finanziell motivierte Insiderhandlungen, wie das Leaken von Patientendaten (Choi et al. 2019, S. 974).

17 Die Groß- oder Kleinschreibung des Begriffsbestandteils ›kritisch‹ fand in der Fachliteratur bisher uneinheitlich statt. Im weiteren Verlauf wird daher die Kleinschreibung bevorzugt.

18 Orye und Maennel propagieren in ihrer Arbeit von 2019 eine »*Encompassing Taxonomy of Cyber Effects*«, die zwischen »*physical*«, »*digital*«, »*economic*«, »*psychological*«, »*political/reputational*« und »*social/societal*« Effekten von Cyberoperationen unterscheidet. Ein ähnlich umfassendes Vorgehen sieht zudem das »*Cyber Harm Model*« der Oxford University vor (Agrafiotis et al. 2016). Für eine Kodierung möglichst vieler Vorfälle, wie sie im Rahmen des HD-CY.CON praktiziert wird, wäre jedoch eine solche Kategorisierung von Cybereffekten aus forschungspragmatischen Gründen heraus nur schwierig bis kaum zu bewältigen. Nur für einen kleinen Teil der öffentlich bekannt gewordenen Angriffe existieren ausreichende Informationen für eine solch graduelle Kodierung, zudem wäre eine Bewertung der ursprünglichen Zielsetzungen der AngreiferInnen (im Gegensatz zu einer hauptsächlichen Erfassung der tatsächlichen Effekte) letzten Ende zumeist nur eine Interpretation.

19 Die nachfolgenden Ausführungen zur Veranschaulichung der Kodierpraxis in Bezug auf die Incident-Types und deren Intensitätsbewertungen basieren auf (Steiger et al. 2018, S. 86–89).

20 Phishing-Operationen stellen den Versuch dar, unrechtmäßigerweise an Daten/Informationen/Zugriffsrechte eines Ziels zu gelangen, indem man sich diesem gegenüber als vertrauenswürdige oder gar bekannte Person/Institution darstellt, z.B. via Phishing-Mails. Social-Engineering bezeichnet jede Form von Manipulation einer Person, die darauf abzielt, durch zumeist nicht-technische Betrugsformen an Daten/Informationen dieser Person zu gelangen. Dabei kann zuvor gesammeltes Wissen über diese Person ausgenutzt werden, oder aber generelles menschliches Fehlverhalten, etwa im Umgang mit E-Mail-Anhängen, aber auch die Hilfsbereit oder Angst einer Zielperson. Social Engineering ist jedoch nicht auf Online-Maßnahmen beschränkt (BSI 2021).

2018; Symantec 2018; UNODC 2019).[21] Zusätzlich können die abgegriffenen Daten in der Folge veröffentlicht (geleakt) werden, was ein Fall von Data Theft + Doxing wäre. Die Kategorie der Disruption beschreibt dagegen einen Cyberangriff, der die Störung einer Funktion oder mehrerer Funktionen des Zielsystems zur Folge hatte. Am häufigsten handelt es sich dabei um DDoS-Angriffe, die die Nichterreichbarkeit des Zielsystems durch Überlastung in Folge von massiv gehäuften Anfragen an den Zielserver bewirken. Ein weiteres Beispiel wäre der Missbrauch des Social-Media-Accounts eines Politikers. Hierbei bedarf es in der Regel keiner anspruchsvollen Hacking-Methoden, zumeist werden lediglich schwach gesetzte Passwörter ausgenutzt oder Phishing-Nachrichten im jeweiligen Netzwerk versendet. Somit wäre dies ein Fall der Disruption, jedoch ohne Hijacking, da hierbei die gestörte Funktionserfüllung des Social-Media-Accounts im Vordergrund stünde. Hijacking bezeichnet dagegen Fälle, in denen es AngreiferInnen gelingt, sich umfassende Zugriffs- und Administratorenrechte auf das jeweilige Zielsystem zu verschaffen. Somit wäre es ihnen in der Folge möglich, diese Rechte auszunutzen und etwa Sabotage oder Spionage zu betreiben. Ein tatsächlicher Missbrauch kann dabei jedoch nicht immer beobachtet werden.[22] Hijacking stellt in gewisser Weise eine (technische) Ergänzungskategorie zu Data Theft und/oder Disruption dar. So wird ein System zumeist gehijackt, um entweder Data Theft oder Disruption als eigentliches Ziel zu ermöglichen. Daher erfasst der HD-CY.CON Hijacking oft in Kombination mit Data Theft und/oder Disruption.

Jede der drei Angriffskategorien kann entweder mit ›1‹ oder ›2‹ hinsichtlich ihrer Intensität bewertet werden. Für Data Theft-Fälle erfolgt diese Unterscheidung anhand der Sensitivität/Vertraulichkeit der abgegriffenen Daten aus Sicht des Opfers. Im Datensatz wird somit nicht die technische Güte der Spionage-Operation, sondern die Klassifizierung der betroffenen Daten hinsichtlich ihrer Bedeutung für das betroffene Ziel als Indikator der Intensität verwendet. Je sensibler/vertraulicher die abgegriffenen Daten, desto schwerwiegender der Angriff. Da hierbei wiederum kein hartes Schwellenwertkriterium zur Anwendung kommen kann, beinhaltet die Kodierung in diesem Fall eine gewisse Interpretationserfordernis seitens des Kodierers oder der Kodiererin, sofern das Opfer selbst oder die jeweiligen Quellen keine eigene Einschätzung hinsichtlich des Vertraulichkeits-/Bedeutungsstatus der Daten liefern. Für staatliche AkteurInnen wird dabei zwischen ›non-classified‹ (1) und ›classified‹ (2) Informationen unterschieden, für private AkteurInnen dagegen zwischen ›non-sensitive‹ (1) und ›sensitive‹ (2) Informatio-

---

21 Watering Hole-Angriffe nutzen hierfür erstellte Fake-Websiten aus, um an die Zugangsdaten adressierter NutzerInnen dieser Seite zu gelangen. Living-Off-the-Land-Operationen missbrauchen zur Infizierung bzw. Ausführung der Schadsoftware bereits auf dem Zielsystem installierte Programme, Apps etc. (Watanabe und Schmitz 2021).

22 Wie Buchanan 2017 richtig feststellt, ist die Unterscheidung zwischen Cyberspionage und vorbereitender Sabotage (also dem Äquivalent ›Hijacking without misuse‹ im HD-CY.CON) äußerst schwierig, insbesondere für das Opfer selbst. Somit dient der technische Sophistizierungsgrad des Angriffes, die Art der verschafften Zugriffsrechte, sowie Kontextfaktoren wie die Charakterisierung des jeweiligen Zieles, als Indikatoren, um dennoch zu einer Bewertung kommen zu können. Dringen mutmaßlich staatliche AngreiferInnen beispielsweise in die Industrial Control Systeme (ICS) eines Stromversorgers und damit kritischer Infrastrukturen ein, ist dieser Fall plausibler als Hijacking (vorerst ohne Misuse) zu bewerten, denn als bloße Cyberspionage.

nen. Auch wenn ein Opfer die Bedeutung der abgegriffenen Daten bewusst herunterspielen könnte, ist dies im Falle fehlender Einschätzungen Dritter die einzige Grundlage für eine Kodierung. Eine bewusst verzerrte Darstellung der Güte der abgegriffenen Daten sollte somit stets in Betracht gezogen werden. Gerade für der Öffentlichkeit/Wählerschaft verpflichtete AkteurInnen oder Institutionen könnte ein solches Vorgehen jedoch zu noch höheren Kosten führen, falls diese Falschdarstellung letztlich doch öffentlich werden sollte.

Im Falle der Disruption-Kategorie wird anhand der zeitlichen Dauer der Funktionsstörung unterschieden. Mehrtägige und darüber hinaus andauernde Störungen werden mit ›2‹ kodiert, während lediglich mehrstündige DDoS-Angriffe mit ›1‹ bewertet werden.[23] Hijacking ohne Misuse wäre die erste Intensitätsstufe der dritten Angriffstyp-Kategorie, während Hijacking mit Misuse deren Steigerung darstellt und somit mit dem Code ›2‹ versehen wird.[24] Zusätzlich zu den jeweiligen Bewertungen des vorgefallenen Angriffstyps erfasst der HD-CY.CON potenzielle physische Auswirkungen in direkter Folge eines Cyberangriffes. Beispielhafte Fälle hierfür wären die Zerstörung der Zentrifugen durch Stuxnet sowie die Stromausfälle in der Ukraine 2015 und 2016 (Farwell und Rohozinski 2011; Brewster 2016b; Greenberg 2019b). Es reicht hierfür nicht aus, wenn etwa ein Computer in Folge eines Angriffes dauerhaft ausgeschaltet bleiben müsste, wenn dessen Hardware dennoch uneingeschränkt funktioniert und der Shutdown lediglich eine Maßnahme zur Eindämmung einer Malware darstellt.[25]

Anhand des Beispiels von Stuxnet soll die Intensitätsbewertung veranschaulicht werden: Die zutreffenden Angriffstypen in diesem Fall wären sowohl Disruption, da die normale Funktionserfüllung der betroffenen Industrial Control-Systeme (ICS) durch den Angriff gestört wurde, als auch Hijacking mit Misuse, da die umfassenden Zugriffsrechte im Sinne der Manipulation der Geschwindigkeit der Zentrifugen ausgenutzt wurden. Da die Störung der betroffenen Nuklearanlage in Natanz der Quellenlage zufolge zudem über mehrere Jahre andauerte, werden sowohl Disruption als auch Hijacking jeweils mit ›2‹ kodiert. Die Zerstörung der Zentrifugen als direkte Folge der Cyberoperation qualifiziert Stuxnet für eine Kodierung der Kategorie ›Physical Effects‹ größer null: Da es lediglich in Natanz zu solch einer zerstörerischen Wirkung durch Stuxnet kam, wird die räumliche Kategorie mit ›1‹ bewertet. Für die Dauer der Disruption wurde stattdessen eine ›2‹ kodiert, da diese länger als einen Tag andauerte. Insgesamt ergibt sich für Stuxnet somit ein ungewichteter Intensitätswert ›7‹. Der angesprochene Target-Multiplier 1,5 würde zudem greifen, da Einschätzungen von IT-Experten zufolge das iranische

23 Gerade im Falle von DDoS-Attacken, der häufigsten Disruption-Angriffsart, stellt die zeitliche Dauer den zumeist am ehesten zu bewertenden und damit konsistentesten Indikator für die Intensität des Angriffes dar.

24 In diesem Fall drückt sich der Misuse zumeist entweder durch Data Theft oder Disruption aus, weshalb hier mehrere Incident-Types vorliegen würden. Hijacking ohne Misuse kann das Infiltrieren fremder Systeme über einen längeren Zeitraum bedeuteten, wobei jedoch nach öffentlichem Kenntnisstand die erlangten Zugriffsrechte (bislang) noch nicht missbraucht wurden (vgl. Errichtung von »*beachheads*« in Zielsystemen, s. Buchanan 2017).

25 Ein Beispiel hierfür wäre die tausendfache Abschaltung von Computern innerhalb der saudi-arabischen Ölfirma Saudi Aramco, als Reaktion auf die Verbreitung der schadhaften Shamoon-Software 2012. Hierbei waren jedoch die ICS-Bestandteile der Ölförderung nicht betroffen (Perlroth 2012).

Atomwaffenprogramm in Folge von Stuxnet um bis zu zwei Jahre zurückgeworfen wurde (Katz 2010), was als Schwächung der offensiven Militärstrategie des Landes gewertet werden kann. Insgesamt ergibt sich somit ein gewichteter Wert von ›10,5‹ für Stuxnet, was bislang als eine Art Ausreißer in maximaler Richtung zu werten ist. Für den Großteil der zu kodierenden Angriffe werden allein aufgrund der nichtvorhandenen physischen Effekte sowie des wohl eher selten greifenden Target-Multipliers Werte zwischen eins und sechs erwartet.

Neben diesen technischeren Analysekriterien erfolgen nun die Beschreibung der Politisierungsmessung und eine Diskussion ihrer Relevanz für die Cyberkonfliktforschung.

4.2.1.3 Politisierung

Neben den Aspekten der Attribution und Intensität der erfassten Cybervorfälle stellt die Kodierung potenzieller Politisierungen einen weiteren Mehrwert des HD-CY.CON dar. Die Frage nach der politischen Adressierung von Cyberangriffen impliziert dabei mehrere theoretisch bedeutsame Komponenten: Zuerst bedeutet die Politisierung ein wichtiges Inklusionskriterium von Cyberoperationen ohne sonstige politische Dimension im Rahmen des Datensatzes. Rein auf finanzielle Gewinne ausgerichtete Cyberkriminalitätsvorfälle, die zudem weder auf ein politisches Ziel gerichtet noch einem politischen Akteur zugesprochen wurden, können und müssen im Falle einer Politisierung nichtsdestotrotz erfasst und kodiert werden, da ihnen durch diesen Akt eine politische Dimension verliehen wird (Steiger et al. 2018, S. 89). Zweitens können auch hier existierende Unterschiede zwischen den Regimetypen untersucht werden. Aufgrund des demokratischen Gebots transparenter Regierungspraxis sowie umfassender Kontrollbefugnisse nichtstaatlicher AkteurInnen ist von einem höheren Maß an Politisierungen von Cyberoperationen in demokratischen Staaten durch die jeweilige Regierung auszugehen als in ihren autokratischen Pendants (Steiger et al. 2018, S. 91). Darüber hinaus stellen sich jedoch weitere Fragen hinsichtlich staatlicher Politisierungspraktiken: Werden diese regelmäßig in besonderem Maße gegenüber bestimmten AngreiferInnen, z.B. ›Enduring Rivals‹, angewandt? Politisieren Regierungen in erster Linie Angriffe auf staatliche oder private Ziele im eigenen Inland? Inkludieren Politisierungen von Cyberoperationen sämtliche Incident-Types oder werden regelmäßig in erster Linie die disruptiveren Formen, etwa Hijacking mit Missbrauch, gepaart mit einer durch physische Schäden besonders hohen Intensität, politisiert? Und zuletzt: Sind es vor allem PolitikerInnen außerhalb der Regierung, die Politisierungen vornehmen, um den Handlungsdruck auf die Regierung in solchen Fällen zu erhöhen, auch hinsichtlich geforderter Attributionen?

4.2.1.4 Beschreibung der übrigen Kategorien des Datensatzes

Nachdem die zentralsten Kategorien des HD-CY.CON-Codebooks vorgestellt und theoretisch plausibilisiert wurden, erfolgt nun eine Zusammenfassung der übrigen Kategorien.[26]

26 Es werden hier wieder nur die inhaltlich bedeutsameren Kategorien vorgestellt, das gesamte Codebook findet sich bei Harnisch et al. 2021.

Die Kodierung der betroffenen Ziele erfolgt analog zur Erfassung des oder der Angreifer(s), somit werden diese in »*Receiver-Category*« sowie »*Receiver-Country*« unterschieden (Steiger et al. 2018: 82):

Tabelle 3: Kategorie ›Receiver-Category‹ HD-CY.CON

Code	Subcode	Beschreibung
0		Unknown
1		State-Institutions/Political System
	1	Government/Ministries
	2	Legislative
	3	Civil Service/Administration
	4	Judiciary
	5	Military
	6	Police
	7	Intelligence Agencies
	8	Political Parties
	9	Election-Infrastructure/Related Systems
	11	Other (e. g. Embassies)
2		International/Supranational Organization
3		Critical Infrastructure
	1	Energy
	2	Water
	3	Transportation
	4	Health
	5	Chemicals
	6	Telecommunications
	7	Food
	8	Finance
	9	Defence-Industry
4		Social Groups
	1	Ethnic
	2	Religious
	3	Hacktivist

	4	Criminal
	5	Terrorist
	6	Human-Rights-Organizations/Activists
	7	Political Opposition/Dissidents/Expats
	8	Other (e. g. NGOs with political goals)
5		Commercial Targets
6		End User(s)
7		Media
8		Science
9		Other

(Eigene Darstellung)
*Mehrfachkodierungen innerhalb eines Falles sind möglich, falls verschiedene Receiver-Categorys im Rahmen eines Angriffes betroffen waren (bis zu zehn Codes).

Entsprechend der verwendeten Konfliktdefinition des HIIK erfasst der HD-CY.CON (wenn möglich) nicht nur Informationen über Opfer, Täter, technische Ausgestaltung und Auswirkung des Angriffes, sondern auch, was die Täter zu ihrem Handeln veranlasst hat. Dieses ›Conflict-Issue‹ ist zentraler Bestandteil der allgemeinen Konfliktmessung des HIIK und sieht dabei folgende Kodieroptionen vor:

Tabelle 4: Kategorie ›Conflict-Issues‹ im HD-CY.CON

Code	Beschreibung
0	No Spillover
1	System/Ideology
2	National Power
3	Autonomy
4	Territory
5	Subnational Predominance
6	Resources
7	International Power
8	Decolonization
9	Secession

10	*(Nur Cyber-Conflict-Issue)*: Cyber-specific*
11	*(Nur HIIK Offline-Conflict-Issue)***: Third-Party-Intervention/Third-Party-Affection

*Im HIIK-Codebook nicht enthalten.
** Im HIIK Codebook nicht enthalten. Wird jedoch zusätzlich zum HIIK Offline-Konfliktgegenstand kodiert, wenn der auf der Cyberebene attackierende Akteur sich in seiner Handlung auf einen HIIK-Konflikt bezieht, bei dem er eigentlich kein Teil der Konfliktdyade ist. Beispiel: Türkische HackerInnen greifen Armenien als Reaktion auf Entwicklungen im Konflikt zwischen Armenien und Aserbaidschan um Bergkarabach an; daraus ergäbe sich folgende Kodierung der HIIK-Offline-Conflict-Issues: Siehe HIIK Konfliktbarometer Dyade Aserbaidschan – Armenien im Startjahr der Cyberoperation + 11.

Die in Tabelle 4 gelisteten Konfliktgegenstände werden jeweils für die Cyberoperation selbst sowie einen potenziell zugrunde liegenden Konflikt kodiert. Für die konventionelle Ebene wird zudem die Intensität der Konfliktdyade des betreffenden Konfliktbarometers im Cyberoperationsstartjahr erfasst. Grundlage hierfür ist jedoch, dass sich die Cyberoperation auch plausibel diesem konventionellen Konflikt und zumindest einem der dabei im Konfliktbarometer angegebenen Konfliktgegenstände zuordnen lässt. Die Kodierung dieses ›Cyber-Conflict-Issue‹ erfolgt entsprechend der vom HIIK aufgestellten Kategorien (Tabelle 4), sieht jedoch an zehnter Stelle die Zusatzkategorie ›Cyber-specific‹ vor. Diese wird kodiert, falls eine Konflikthandlung ohne die Existenz des Cyberspace nicht möglich bzw. nötig wäre. Ein Beispiel hierfür wären DDoS-Attacken seitens HacktivistInnen gegen eine Regierung, die zuvor Internetzensurmaßnahmen verhängt hat.[27]

Die Kategorie ›Zero-Days‹ gibt ferner an, ob Informationen über die Verwendung von einem (›2‹) oder mehreren (›2,1‹) Zero-Day-Exploits vorliegen. Wie bereits erläutert, werden diese speziellen Sicherheitslücken in erster Linie von sophistizierten, mit entsprechenden Ressourcen ausgestatteten AkteurInnen verwendet, da deren ›Finden‹ zumeist bereits eine Herausforderung darstellt (Steiger et al. 2018, S. 84). Somit kann über die Erfassung verwendeter Zero-Days eine Attribution potenziell gestützt oder auch zumindest in Zweifel gezogen werden. Nutzt beispielsweise eine APT, der staatliche Unterstützung nachgesagt wird, einen Zero-Day-Exploit im Zuge der Attacke, so könnte dies die Attribution stützen, da in erster Linie staatlichen Behörden und AkteurInnen deren Sammlung und Verwendung nachgesagt werden. Da diverse Zero-Days jedoch bereits länger im Internet kursieren,[28] aufgrund unzureichender Patching-Praktiken der AnwenderInnen der Zielsysteme jedoch immer noch erfolgreich ausgenutzt werden können, ist eine derartige Schlussfolgerung stets mit Bedacht zu ziehen, was im Rahmen dieser Arbeit nur in besonders plausiblen Fällen erfolgt.[29] Die Malware Stuxnet, bei der

27 In einem solchen Fall würde zusätzlich ›System/Ideology‹ als Cyber-Conflict-Issue kodiert werden.
28 Die gängige Bezeichnung hierfür lautet »*in the wild*« (Osborne 2020).
29 Das sog. »*Common Vulnerability Scoring System*« (Mell et al. 2007) stellt einen möglichen Indikator für die jeweilige Charakterisierung der Sicherheitslücken dar.

vier verschiedene, ›echte‹ Zero-Days ausgenutzt wurden, kann auch in diesem Fall als exemplarisch angesehen werden, da hierdurch die Attribution in Richtung amerikanischer und israelischer Geheimdienste untermauert wurde.

4.2.2 Allgemeine Kennzahlen zum Datensatz im Vergleich

Der HD-CY.CON zeichnet sich (wie in Tabelle 5 dargestellt) durch eine weitaus umfassendere Datenbasis aus als die beiden bekanntesten Alternativ-Datensätze. So verzeichnet er 1265 Cyberoperationen für die Jahre 2000–2019. Im Falle des DCID (1.5) sowie des CFR-Tracker sind es weitaus weniger erfasste Fälle, was sich teilweise aus dem engeren Fokus auf staatliche/staatlich gesponserte AngreiferInnen ergibt. Auch wenn der HD-CY.CON für Cyberoperationen mit staatlicher Beteiligung mit 512 erfassten Fällen unter der Zahl des CFR-Trackers liegt (siehe Abschnitt 5.2.1), bietet er dennoch insgesamt die umfassendere Datenbasis: So erfasst der HD-CY.CON aufgrund einer differenzierteren Attributionskodierung in anderen AngreiferInnen-Kategorien diverse Fälle, die vom CFR-Tracker als staatlich gesponsert erfasst wurden, etwa wenn die öffentliche Quellenlage entgegen der Kodierung des CFR-Trackers keine staatliche Unterstützung der Operation suggeriert.

Tabelle 5: Vergleich politikwissenschaftlicher Cyberkonfliktdatensätze

Datensatz	Zeitraum (Startjahr)	Erfasste Fälle*	Kodierintervall
HD-CY.CON	2000 – 2019	1265	Jährlich
DCID (1.5)	2000 – 2016	266	Unregelmäßig (mehrere Jahre)
CFR Tracker	2005 – 2020	541	Vierteljährlich

(Eigene Darstellung), *Stand: November 2021

4.3 Theoriegeleitete Fallauswahl mithilfe deskriptiver Statistik

Entsprechend eines ›sequenziell quantitativ-qualitativen‹ Designs folgt auf den quantitativen Untersuchungsteil im Sinne einer deskriptiven Auswertung des HD-CY.CON zur Durchführung der Fallauswahl ein strukturierter, fokussierter Vergleich als qualitativer Forschungsschritt (Kelle 2014, S. 161). Dabei wird die jeweilige Bedeutung der Forschungsteile gleich gewichtet (Kelle 2014, S. 160): Obwohl ein strukturierter Vergleich auch ohne die umfangreiche Auswertung eines Large-n-Datensatzes durchgeführt werden kann, wären seine Repräsentativität und Validität im Sinne der Fallauswahl begrenzt. Der HD-CY.CON-Datensatz reduziert somit empirische ›blinde Flecken‹, die die Fallauswahl verzerren könnten. Die Kombination aus quantitativer Häufigkeitsanalyse und qualitativ strukturierter, vergleichender Analyse soll dazu dienen, die vermutete Beziehung zwischen Regimetyp und Proxy-Nutzung in einem bislang unterentwickelten Forschungsgebiet ohne ausreichende Grundlagenforschung zu untersuchen (Kelle

2014, S. 153). Dies gilt noch stärker für die konzeptualisierte defensive Cyberproxy-Nutzung demokratischer Staaten.

Nach der statistischen Beschreibung des Datensatzes werden jeweils zwei Fälle für Autokratien und Demokratien ausgewählt: Unter einem ›Fall‹ werden im Kontext der Arbeit ein Land und dessen Proxy-Nutzung/Beziehung im Untersuchungszeitraum verstanden. Für die Gruppe der Autokratien sollen somit Varianzen in Art und Funktion der prävalenten Proxy-Nutzung aufgezeigt und erklärt werden.[30] Daher gilt es, zwei besonders häufig und intensiv Cyberproxys nutzende Autokratien aus dem Datensatz herauszufiltern, denen dennoch zusätzlich eigene staatliche Cyberangriffe zugesprochen wurden, um den potenziellen Aspekt der Plausible Deniability als primäres Motiv zur Proxy-Nutzung noch stärker untersuchen zu können.[31] Zweitens können somit auch zeitliche Varianzen in der Proxy-Nutzung gegenüber allgemein/direktstaatlich attribuierten Cyberoperationen eher identifiziert werden, was beispielsweise auf die bewusste Entmachtung einer staatlichen Institution durch die zeitweilige Instrumentalisierung von Proxys hindeuten könnte.

Die beiden Autokratien sollten hinsichtlich der anvisierten Ziele der Angriffe, der angewandten Incident-Types sowie des autokratischen Subtyps regelmäßige Unterschiede aufweisen. Darüber hinaus ist eine möglichst große zeitliche Abdeckung des Datensatzes seitens der Länder erstrebenswert: Je mehr Daten für die ausgewählten Autokratien vorliegen, desto fundierter können die anschließenden Fallstudien wiederum durch den HD-CY.CON gestützt werden. Durch die exemplarische Analyse besonders häufig eingesetzter Proxy-Gruppierungen kann somit im vergleichenden Untersuchungsdesign die bereits im Datensatz angelegte Längsschnittkomponente im Sinne einer potenziellen ›Within-Case-Variance‹ noch expliziter analysiert werden (Levy 2008, S. 10). Für die abhängigen Variablen des Analysemodells steht somit im Kontext der Fallauswahl der Aspekt der Funktion der Proxys notwendigerweise zunächst im Vordergrund, da dieser im Gegensatz zur Art direkt aus dem Datensatz abgelesen werden kann. Nichtsdestotrotz wird bei der Fallauswahl auch darauf geachtet, ob die beiden favorisierten Autokratien hinreichende Unterschiede hinsichtlich ihrer Involvierung in gewaltsame konventionelle Konflikte und somit der Ausprägung der IV aufzeigen, wie sie der HD-CY.CON im Rahmen der HIIK-Offline-Issue/Intensity-Kategorien erfasst.

---

30 Somit soll aus methodologischer Sicht ein »*no-variance-design*« hinsichtlich der beiden AVs vermieden werden (King et al. 1994, S. 128–139). Eine vorhandene offensive, respektive defensive Cyberproxy-Nutzung wird jedoch als Voraussetzung für die Fallauswahl angenommen, »*variance*« bedeutet hier somit *nicht* die dichotome Konstellation ›Cyberproxy-Nutzung‹ vs. ›keine Cyberproxy-Nutzung‹.

31 Allgemein/direktstaatlich attribuierte Cyberoperationen der beiden Autokratien dienen somit in gewisser Weise als Kontrollfälle, um das autokratische Grund-Motiv für offensive Cyberproxy-Nutzung im Generellen systematischer für den jeweiligen Fall herausarbeiten zu können. Würden nur Autokratien mit ausschließlich kodierten Proxy-Operationen untersucht werden, könnten die Motive der Plausible Deniability, sowie des Coup Proofings nicht hinreichend auf ihre Erklärungskraft getestet werden, da in solchen Fällen fehlende staatliche Kapazitäten zur Durchführung eigener Cyberoperationen am plausibelsten erscheinen (unter der Bedingung eines grundlegenden Interesses hieran) und die beiden anderen genannten Motive, wenn, dann eher als Sekundärmotive einzustufen wären.

Auf demokratischer Seite kann, wie bereits beschrieben, eine Fallauswahl aufgrund der US-amerikanischen Suprematie im Technologiesektor eigentlich nur über die Vereinigten Staaten als ›Most-Likely-Case‹ erfolgen. Entsprechend der Auswertung des HD-CY.CON soll jedoch überprüft werden, ob es andere Demokratien gibt, die bereits ähnliche Proxy-Nutzungspraktiken demonstriert haben. Denkbar wären hier etwa Großbritannien und Israel aufgrund ihrer Stärke im privatwirtschaftlichen IT-Sektor. Die am zweithäufigsten durch nationale IT-Firmen attribuierende Demokratie des Datensatzes wird somit den USA als Vergleichsfall zur Seite gestellt. Ist deren Attributionshäufigkeit des IT-Sektors im Gegensatz zu den nachfolgend platzierten Demokratien vergleichsweise gering, wird als weiteres Kriterium die Anzahl an erfassten IT-Unternehmen ausgewählt. Für einen hinreichend geeigneten Vergleichsfall mit den USA erscheint z.B. ein Land mit nur einer im Datensatz vertretenen IT-Firma weniger geeignet als ein Land mit größerer Diversität in diesem Bereich.

Ließen sich außer für die USA keine derartigen Attributionsmuster auf Seiten einer weiteren Demokratie erkennen, läge die Vermutung nahe, dass es sich bei der konzeptualisierten defensiven Cyberproxy-Nutzung eher um eine US-spezifische Anomalie als um ein allgemein demokratisches Phänomen handeln könnte. Im Falle demokratischer Cyberproxy-Nutzung wird an dieser Stelle deutlich, dass die im Rahmen der Arbeit durchgeführte Konzeptualisierung durch weniger theoretische sowie empirische Vorarbeiten gestützt wird als im Falle klassischer, autokratischer Cyberproxy-Nutzung. Somit kommt der Fallauswahl auf demokratischer Seite eine etwas andere Rolle zu als auf autokratischer Seite. Für Autokratien erscheint die These der offensiven Cyberproxy-Nutzung bereits vor der Analyse als wahrscheinlich, daher wird hier der Fokus auf Varianzen innerhalb der jeweiligen Strategie (AVs) gelegt. Im Falle der Demokratien gilt es hingegen, zunächst die These der defensiven, attributionsbasierten Proxy-Nutzung *per se* zu überprüfen. Etwaige Varianzen innerhalb dieser stellvertretenden Attributionen sollen dagegen stärker im Laufe der empirischen Analyse herausgearbeitet und für eine potenzielle Anpassung der Ursprungshypothesen genutzt werden. Ein weiterer demokratischer Vergleichsfall, dessen Attributionskodierungen ebenfalls auf eine defensive Cyberproxy-Nutzung schließen lassen, könnte somit das theoretische Argument erhärten bzw. im Hinblick auf potenzielle, intrademokratische Varianzen weiter ausdifferenzieren und somit zur Weiterentwicklung des Erklärungsmodells beitragen.

Konkret wird zunächst auch aufseiten der Demokratien durch Zuhilfenahme deskriptiver Statistik ermittelt, ob die getätigten Hypothesen bezüglich einer grundlegend niedrigeren bis kaum vorhandenen offensiven Proxy-Nutzung im Cyberspace auf Grundlage der Daten zu bestätigen sind. Ist dies der Fall, wird für die propagierten, defensiveren demokratischen Cyberproxys eine Häufigkeitsanalyse der kodierten Länder, aus denen die jeweils attribuierenden IT-Firmen stammen (Variable ›Country of Origin: IT-Attribution‹), vorgenommen. Verglichen werden die beiden am häufigsten kodierten Länder sodann mit den in den betreffenden Fällen kodierten Receiver-Countrys. Um als relevanter Fall auf demokratischer Seite gelten zu können, müssten hierbei regelmäßige Übereinstimmungen zu finden sein.

Tabelle 6 verdeutlicht die Schwerpunktlegung auf die variante Ausprägung der AVs im Falle der Autokratien sowie die zunächst dichotom positive Ausprägung der AVs im Falle der Demokratien mit dennoch potenziell herauszuarbeitenden Varianzen.

Tabelle 6: Schematische Darstellung des Vorgehens der Fallauswahl

	AV I	AV II	UV	KV	IV
Autokratien	*Positiv/Varianz*	*Positiv/Varianz*	?	?	?
Demokratien	*Positiv/Varianz möglich*	*Positiv/Varianz möglich*	?	?	?

(Eigene Darstellung)

4.4 Konzeptoperationalisierung im Rahmen eines strukturiert-fokussierten Vergleiches

Der angestrebte Ansatz des »*structured-focussed comparison*« (SFC) wird seitens seiner Entwickler George und Bennett wie folgt beschrieben:

> »The method and logic of structured, focused comparison is simple and straightforward. The method is ›structured‹ in that the researcher writes general questions that reflect the research objective and that these questions are asked of each case under study to guide and standardize data collection, thereby making systematic comparison and cumulation of the findings of the cases possible. The method is ›focused‹ in that it deals only with certain aspects of the historical cases examined. The requirements for structure and focus apply equally to individual cases since they may later be joined by additional cases.« (George und Bennett 2005, S. 67)

Der gewählte Ansatz lässt sich somit ebenfalls als theoriegeleitetes Process-Tracing im Rahmen eines Small-n-Vergleiches beschreiben. Auch wenn keine vergleichbare Generalisierbarkeit wie im Falle statistischer Large-n-Untersuchungen erreicht werden kann, erlaubt dieses Vorgehen durch die erreichte Analysetiefe die Bewertung komplexer kausaler Prozesse, da dies in stetiger Verbindung mit den theoretisch hergeleiteten Annahmen erfolgt (Hall 2003, 391–392). Die genuinen Charakteristika des Cyberspace, z.B. das hohe Maß an Geheimhaltung und verdeckten Operationen sowie das allgemein eher geringe Maß an politischer Transparenz, erfordern eine qualitative Untersuchung der beschriebenen UV, IV und KV. Dagegen können die AVs durch den HD-CY.CON hinsichtlich der Fallauswahl statistisch erhoben und ausgewertet werden. Jedoch gebietet auch bei ihnen die nachgelagerte Bewertung der jeweils fallbezogenen Ausprägungen die Anreicherung durch qualitativ erhobene Indikatoren zur umfassenden Beschreibung der Proxy-Funktionen und -Typen.

Im Rahmen des SFC folgt der/die WissenschaftlerIn folgenden fünf Arbeitsschritten (Bennett 2004, S. 32–33):

1. Spezifizierung der Forschungsfrage,
2. Definieren der UV, AV und IV,
3. Auswahl und Vergleich der Fallstudien,

4. Operationalisierung der Variablen-Ausprägungen sowie
5. Formulieren der jeweils strukturierenden Forschungsfragen.[32]

Die Schritte 1 und 2 wurden bereits in den vorherigen Kapiteln durchgeführt und beschrieben.[33] Da die Auswahl und der Vergleich der Fallstudien erst nach der Analyse des HD-CY.CON erfolgen können, gilt es nun, die Variablen des Kausalmodells zu operationalisieren und anschließend die Forschungsfragen für die Fallstudien zu formulieren. Bei der Operationalisierung der Konzepte der zu untersuchenden Variablen sollen entsprechend des ontologischen Ansatzes von Gary Goertz neben theoretischen Erwägungen auch empirische Beobachtungen in die Spezifizierung einfließen. Nur so könne verhindert werden, dass Konzeptdefinitionen und deren empirische Analyse einzig nach Belieben der jeweilig gewählten Definition des Forschers willkürlich konstruiert werden. Die zentralen Attribute eines Konzeptes seien somit jene, die besondere Relevanz für deren Verwendung und Analyse im Rahmen von Hypothesen und Kausalmodellen aufweisen (Goertz 2012, S. 4). Dies stellt zudem den Nexus zur Analyseeinheit der »*causal-process observations*« (CPOs) her, »*an insight or piece of data that provides information about context, process, or mechanism, and that contributes distinctive leverage in causal inference*« (Collier et al. 2004, S. 252). Somit werden nicht nur standardisierte »*data-set observations*« (DSOs) des HD-CY.CON analysiert (Collier et al. 2004, S. 252), sondern auch nicht standardisierbare CPOs, die dennoch einen hohen Nutzen im Rahmen des Process-Tracings besitzen (Mahoney 2010, S. 127).

4.4.1 Funktionen autokratischer Cyberproxys

Gemäß der Verwendung des HD-CY.CON werden die verschiedenen *Funktionen* (AV I) und somit die Zwecke des autokratischen Cyberproxy-Gebrauchs in erster Linie über den jeweils angewandten Incident-Type im Rahmen offensiver Cyberoperationen operationalisiert (Data Theft, Disruption, Hijacking; siehe 4.2.1.2). Jedoch kann etwa Datendiebstahl ökonomisch, militärisch oder politisch motiviert sein und somit unterschiedliche Funktionen für den staatlichen Auftraggeber erfüllen. Entscheidend wäre für die Funktionsbeurteilung, das Profil der Ziele sowie (falls öffentlich bekannt) der abgegriffenen Daten zu kennen. Die genaue Identität der Täter (AV II) kann darüber hinaus weitere Anhaltspunkte für die Bewertung der intendierten Funktion des Proxy-Einsatzes liefern. So könnte etwa die Infiltration kritischer Infrastrukturen seitens militärisch geführter Proxys als Vorbereitung eines Sabotageaktes (Hijacking plus Misuse) im Rahmen eines konventionellen Konfliktes interpretiert werden, während dasselbe Vorgehen von zivilgeheimdienstlich geleiteten Proxys in Abstinenz eines konventionellen Konfliktes lediglich

32 »These questions must be carefully developed to reflect the research objective and theoretical focus of the inquiry. The use of a set of general questions is necessary to ensure the acquisition of comparable data in comparative studies. […] The important device of formulating a set of standardized, general questions to ask of each case will be of value only if those questions are grounded in – and adequately reflect – the theoretical perspective and research objectives of the study« (George und Bennett 2005, S. 69).

33 Als ›class of events‹ wäre im Rahmen der Arbeit staatliche Cyberproxy-Nutzung zu verstehen.

als allgemeine Aufklärungstätigkeit gewertet werden könnte. Disruption kann dagegen ein allgemeines Signalisieren der eigenen Fähigkeiten oder eine zielgerichtete Maßnahme im Rahmen eines konventionellen Konfliktes darstellen.

In der Literatur wird an dieser Stelle oftmals kritisch vermerkt, dass die tatsächliche Intention von CyberangreiferInnen nur schwer zu beurteilen und diese Bewertung anfällig für menschliche Fehlschlüsse ist (Libicki 2018, S. 118). Der letztliche Zweck von Datendiebstahl ist hierfür das prägnanteste Beispiel. In dieser Arbeit wird jedoch argumentiert, dass gewisse Muster bzw. Varianzen in der faktisch sichtbaren Anwendung von Proxys im Zeitverlauf dennoch Hinweise darauf sein können, welche Funktionen und Ziele hiermit erreicht werden sollten. Ändert eine Autokratie ihre Cyberproxy-Nutzung beispielsweise aufgrund einer erfolgten Eskalation in Folge einer Infiltrierung kritischer Infrastrukturen, so kann dies als Zeichen gewertet werden, dass das eigene Entdeckt werden nicht Teil des ursprünglichen Plans war, sondern dass in erster Linie Informationen gesammelt werden sollten. Wird eine Autokratie dagegen bei einem solchen Vorgehen in Gestalt ihres Proxys überführt, nutzt denselben Akteur jedoch auch in der Folge auf ähnliche Zielsysteme, kann von einem intendierten Signaling-Effekt der eigenen Fähigkeiten ausgegangen werden, ohne diese notwendigerweise auch final zur Anwendung bringen zu müssen.[34] Ob der tatsächliche Missbrauch der Zugriffsrechte zu einem Zeitpunkt tatsächlich geplant war, kann dabei ohne Insider-Kenntnisse nur schwer beurteilt werden. Wahrscheinlicher erscheint dies jedoch, falls sich die Autokratie mit dem jeweiligen Land bereits in einem gewaltsamen konventionellen Konflikt befindet oder sich dieser zumindest bereits andeutet.

Zusammenfassend dient als Hauptindikator für die autokratischen Cyberproxy-Funktionen deren jeweils angewandter Incident-Type, der jedoch im Sinne einer kontextuellen Attribution zu den jeweils anvisierten Zielen sowie den attribuierten AkteurInnen in Beziehung gesetzt werden muss.

4.4.2 Arten autokratischer Cyberproxys

Die institutionelle Anbindung autokratischer Cyberproxys bzw. deren Art kann dagegen aus dem HD-CY.CON über die Kategorie ›Name-Initiator‹ operationalisiert werden. Darin werden sowohl potenzielle Bezeichnungen der attribuierten AngreiferInnen als auch bekannte Affiliationen zu konventionellen Akteuren, etwa zu dahinter vermuteten Unternehmen, aber vor allem auch staatlichen Einheiten, kodiert.[35] Hierüber können Aussagen über die Häufigkeit der jeweils vermuteten institutionellen Anbindung offensiver Cyberproxys erfolgen, die jedoch für eine umfassende Bewertung durch qualitative Primär- und Sekundärquellen ergänzt werden müssen. Diese können Aufschluss darüber liefern, welchem Teil der Winning Coalition sich einzelne staatliche Einheiten zuordnen lassen und inwiefern sich deren strategische Eigeninteressen sowie ihr Herrschaftszugang über die Zeit verändert haben könnten. Sofern es die Datenlage zulässt,

34 Zudem impliziert dieser Fall, dass die entsprechende Attributionspraxis des betroffenen Staates dessen Verwundbarkeit gegenüber dem autokratischen Cyberangreifer offensichtlich nicht effektiv reduziert hat, im Falle einer erfolgreichen Infiltration.

35 Beispiel: Name Initiator I: Charming Kitten; Name Initiator II: IRG (iranische Revolutionsgarden).

soll zusätzlich eine Bewertung einzelner Cyberoperationen entsprechend des Analyserasters zu staatlicher Verantwortlichkeit im Cyberspace von Jason Healey (2011) vorgenommen werden, die durch den HD-CY.CON in ihrer Granularität nicht erfasst werden kann (2011, S. 59–61):

Tabelle 7: Das Spektrum staatlicher Verantwortlichkeit im Cyberspace

Kategorie*	Beschreibung
State-ignored	Der Staat weiß von den Aktivitäten privater AkteurInnen, lässt diese jedoch gewähren.
State-encouraged	Der Staat liefert privaten AkteurInnen ideelle/rhetorische Unterstützung, billigt deren Aktionen und ruft zu Nachahmungen auf.
State-shaped	Der Staat liefert privaten AkteurInnen informelle Unterstützung, etwa durch die Koordination mit gleichgesinnten AkteurInnen innerhalb der Regierung, die außerhalb ihrer Dienstzeit ähnliche Hacks ausführen.
State-coordinated	Der Staat unterstützt private AkteurInnen durch die Auswahl der Ziele, der zeitlichen Abläufe sowie operativer Details. Auch technische Unterstützung ist möglich.
State-ordered	Der Staat unterstützt private AkteurInnen vollumfänglich, ohne diese bereits de facto zu StaatsagentInnen gemacht zu haben.
State-rogue-conducted	Staatliche AkteurInnen führen ohne das Wissen oder gegen den Willen der Regierung Cyberaktionen durch.
State-integrated	Private AkteurInnen werden in staatliche Cybereinheiten integriert. Die Befehle und Koordination können dabei formell oder informell sein, jedoch hat der Staat stets die Kontrolle über die Zielauswahl sowie die operativen Details.
State-executed	Staatliche Cybereinheiten führen Cyberoperationen unter direkter Kontrolle der staatlichen Führung durch.

Quelle: Jason Healey (2011, S. 59–61)
*Es werden hier nur acht der insgesamt zehn Kategorien ausgewählt, da die beiden passivsten Verantwortungsformen (›state-prohibited‹ und ›state-prohibited but inadequate‹) dem hier verwendeten Proxy-Konzept nicht mehr entsprechen.

4.4.3 Funktionen demokratischer Cyberproxys

Aufgrund der zentralen Funktion defensiver Cyberproxys im Sinne der Attribution können auf demokratischer Seite Varianzen standardisierter DSOs nur eingeschränkt direkt aus dem Datensatz herausgelesen werden, weshalb hier CPOs von noch zentralerer Bedeutung sind. So zeigte die Konzeptualisierung der demokratischen AV I, dass auch die spezifischere Funktion technischer Attributionen variieren kann. Entsprechend der diskutierten Legitimations- und Resilienzfunktionen sowie dem allgemeinen Ziel der Reduzierung politischen Handlungsdrucks stellvertretender Attributionen soll vor allem deren Beziehung zu entweder nicht vorhandenen oder zeitlich vor- oder nachgelagerten

politischen Attributionen untersucht werden. Hierfür sind als Indikatoren vor allem die HD-CY.CON-Kategorien ›Source-Incident-Detection/Disclosure‹, ›Temporal Attribution-Sequence‹ sowie die bereits erwähnten ›Attribution-Basis‹ und ›Attribution-Type"[36] dienlich. Erstere gibt dabei an (falls möglich), durch welchen Akteur der jeweilige Vorfall in erster Instanz öffentlich gemacht wurde, unabhängig von einer Attribution. So könnte eine gehäufte Kodierung von IT-Firmen für eine angestrebte Resilienzfunktion sprechen, die mit ihren technischen Berichten einhergeht. Die zweite Kategorie reflektiert dagegen, in welcher Reihenfolge die Attributionen im Falle sowohl vorliegender technischer als auch politischer Attributionen erfolgt sind. Dies könnte somit ein Hinweis darauf sein, ob a) demokratische Regierungen tatsächlich regelmäßig auf private Attributionen bauen, um zunächst den eigenen Handlungsdruck zu reduzieren, b) zuerst veröffentlichte IT-Berichte eine nachgelagerte, politische Attribution ohne umfangreiches Offenlegen eigener Evidenzen ermöglichen, oder c) zuerst erfolgte politische Attributionen durch nachgelagerte technische Attributionsberichte mehr Glaubwürdigkeit erlangen können.[37]

4.4.4 Arten demokratischer Cyberproxys

Die Operationalisierung der Art demokratischer Cyberproxys (AV II) ergibt sich dagegen entsprechend ihrer Konzeptualisierung aus der Erfassung der Kategorie der ›Attribution-Basis‹ sowie des ›Country of Origin: IT-Attribution‹ in Kombination mit dem jeweiligen ›Receiver-Country‹ und bedarf dementsprechend an dieser Stelle keiner weiteren Ausführung.

4.4.5 Domestische Präferenzkonstellationen

Die Operationalisierung der domestischen Präferenzkonstellationen als Haupterklärungs-variable für außenpolitisches Handeln im neuen Liberalismus gestaltete sich bislang relativ wenig formalisiert und divers, eine Art ›Goldstandard‹ scheint noch nicht zu existieren. Erklären lässt sich dies jedoch vor allem auch durch ihre Varianz von Land zu Land und besonders von Regimetyp zu Regimetyp, entsprechend des aufgezeigten Einflusses der republikanischen Ebene sowohl auf den Herrschaftszugang domestischer AkteurInnen als auch auf den konkreten Transfer ihrer Interessen auf die politische Ebene. Dass dabei auch autokratische Subtypen wie Einparteien-Regime wegen grundlegender Ähnlichkeiten zu Demokratien auf der republikanischen Ebene dieselben Kooperationsanreize im wirtschaftlichen Bereich wie diese besitzen können, verdeutlicht nochmals die Interdependenz der drei Liberalismus-Stränge (Mattes und Rodríguez 2014). Prinzipiell sind für die Operationalisierung der UV besonders die

---

36 In ihrer Dissertation von 2021 identifiziert auch Lee vier unterschiedliche »*channels*« der bisherigen US-Attribution (»*technical, criminal, official and unofficial policy*«), die ebenfalls auf die Differenzierung unterschiedlicher Attributionstypen abzielen.

37 Da die defensive Cyberproxy-Nutzung per se und somit auch besagte potenzielle Varianzen hierbei als weniger »*certain*« (Rohlfing 2014, S. 609) angesehen werden als im Falle autokratischer Cyberproxy-Nutzung, werden sie wie bereits beschrieben für die demokratische Fallauswahl auch als nicht zwingend notwendig erachtet.

Interessen von »*politicians, bureaucrats, organized interests, think tanks, NGOs, and voters*« von Bedeutung (da Conceição-Heldt und Mello 2016). Für die Erklärung des außenpolitischen Handelns wird es somit im ersten Schritt wichtig sein, herauszuarbeiten, welche dieser AkteurInnen durch ihren Herrschaftszugang auf republikanischer Ebene im jeweiligen Untersuchungszeitraum für das autokratische oder demokratische Land als besonders relevant erachtet werden können. In der Folge gilt es aufzuzeigen, zu welchen Präferenzkonstellationen gegenüber dem autokratischen oder demokratischen Gegenüber deren Interessen letztlich auf außenpolitischer Ebene führten bzw. geführt hätten, sofern durch den Einsatz des jeweiligen Cyberproxys diese potenzielle Verwundbarkeitsasymmetrie nicht zum eigenen Vorteil hätte gestaltet werden können/sollen. Die republikanische Ebene determiniert somit, welche ideellen und kommerziellen Interessen welcher AkteurInnen sich überhaupt auf politischer Ebene durchsetzen können. Für Demokratien wird aufgrund des zumindest in der Theorie funktionierenden Transmissionsriemens von einer größeren Vielfalt an potenziell hierfür in Frage kommenden AkteurInnen ausgegangen, abhängig vor allem auch vom jeweiligen Zeitkontext. So dürften WählerInnen im Wahlkampfzeitraum einen stärkeren Herrschaftszugang besitzen als kurz nach einer Wahl. Für Autokratien werden in erster Linie die jeweiligen Mitglieder der Winning Coalition und deren Präferenzen als zentral angesehen. Jedoch bedingt der autokratische Subtyp auch hier eine regelmäßige Varianz der Interessensdurchsetzungen unterschiedlicher Elitengruppen.

Auf demokratischer Seite gilt es somit noch stärker aufzuzeigen, welche Interessen welcher domestischen AkteurInnen für die seitens der Autokratie anvisierten Vulnerabilitätsasymmetrie in erster Linie verantwortlich gemacht werden können. Durch das Aufbrechen des Three-Image-Paradigmas der internationalen Beziehungen wird im neuen Liberalismus zudem der Einfluss von Dynamiken und Prozessen der internationalen Ebene auf diese domestischen Präferenzkonstellationen nachgezeichnet.[38] Diese könnten wiederum im Falle von Demokratien durch den in Folge einer Wahl veränderten Herrschaftszugang der AkteurInnen auf politischer Ebene gewandelte Präferenzen auf ideeller und/oder wirtschaftlicher Ebene nach sich ziehen.

Für die Analyse ideeller Präferenzen werden Primärquellen, z.B. staatliche Strategiepapiere, White Paper, Pressemitteilungen oder sonstige Äußerungen der jeweiligen Regierung bzw. bestimmter Teile der Winning Coalition als Indikatoren herangezogen, die über die Wertvorstellungen einer bestimmten Akteursgruppe Auskunft geben.[39] Stellungnahmen in Medienartikeln spielen jedoch auch eine bedeutende Rolle. Hinzu kommt die Analyse von Sekundärliteratur, in der bereits eine umfassende Auseinandersetzung mit der Analyse staatlicher Präferenzentwicklung auf (u.a.) ideeller Ebene für verschiedene Staaten stattfand. Für das Nachzeichnen wirtschaftlicher Präferenzen

38 Bedeutend ist in diesem Kontext auch der Effekt der »*social embeddedness*«, die »*may take the form of fixed investments by private firms, ideological commitments by political parties concerned about their reputation, costly institutional adaptation by domestic bureaucracies, or government investment in military defense*« und somit durch soziale »*lock-in*«-Effekte zu stabilen, staatlichen Präferenzen führen könne (Moravcsik 1997, S. 537).

39 Für cyber-spezifische Präferenzen könnten hierfür auch die dominanten und zunehmend veröffentlichten Cybersicherheits-Doktrinen auf staatlicher Ebene erfasst werden (Lewis 2014).

können dagegen auch stärker quantitative Messzahlen erfasst werden, die beispielsweise die wirtschaftspolitischen Tendenzen eines Landes sowie der darin dominanten AkteurInnen widerspiegeln. Aber auch allgemeine Verschiebungen innerhalb der Haushaltsentwürfe nationaler Regierungen können entsprechend des Prinzips ›Money is Policy‹ als mögliche Indikatoren für veränderte Präferenzkonstellationen in bestimmten Bereichen herangezogen werden (Adams und Williams 2010, S. 1).

Zuletzt wird der Einfluss der republikanischen Ebene besonders durch Bewertungen der verfassungsrechtlichen, institutionalistischen Strukturen des jeweiligen Landes im Untersuchungszeitraum erfasst. Ebenfalls wird erhoben, welche Varianzen darin zum Erstarken bestimmter AkteurInnen und deren Präferenzen geführt haben. Da in der vorliegenden Arbeit der autokratische und demokratische Subregimetyp als Teile der Konzeptualisierung der UV begriffen werden, werden diese wie folgt für die empirische Analyse operationalisiert:

Zur Konzeptualisierung autokratischer Subregimetypen wird die Typologie von Kailitz (2013) herangezogen: Dessen Ansatz liegt dabei die Frage nach der jeweiligen Legitimationsquelle autokratischer Regime für deren Ausdifferenzierung zugrunde. Die Unterscheidung zwischen liberalen Demokratien, elektoralen Autokratien, kommunistischen Ideokratien, Einparteien-Autokratien, Militärregimen, Monarchien und personalistischen Autokratien wird für das Forschungsinteresse der Arbeit aus zwei Gründen als besonders geeignet erachtet: Erstens sind hierdurch feingliedrigere Unterscheidungen hinsichtlich des Einflusses des Subregimetypus auf die republikanische sowie ideelle Ebene domestischer Interessenskonstellationen möglich. Wie Geddes et al. 2014 feststellten, entscheidet nicht nur die bloße Größe der Winning Coaltion/Leadership-Group über deren Handeln, sondern neben diesem formal-republikanischen Charakteristikum auch deren jeweilige Interessenslage. Somit sollten bei der Betrachtung unterschiedlicher autokratischer Subtypen nicht nur Weite und Enge des jeweiligen Herrschaftszugangs betrachtet werden, sondern auch deren Interessen auf ideeller sowie wirtschaftlicher Ebene, was gleichzeitig den Subregimetyp als Teil der UV begründet. Den Aspekt der Legitimation als Hauptunterscheidungskriterium zu wählen, ermöglicht dabei zweitens, die in Abschnitt 2.2.3 aufgezeigten Asymmetrien im autokratischen Herrschaftszugang nach innen und außen enger an die unterschiedlichen Subtypen anzubinden. Wie bereits diskutiert wurde, unterscheiden sich Autokratien besonders in ihrem Modus der eigenen längerfristigen Interessensdurchsetzungschancen gegenüber der domestischen, aber auch außenpolitischen Ebene. Da für den Cyberspace hierbei der Aspekt der Legitimation als immer bedeutsamer charakterisiert wurde, sollte die Konzeptualisierung autokratischer Regimetypen diesen theoretischen Aspekt auch entsprechend abbilden. Das Konzept der Legitimation ist zudem im Gegensatz zu den weiteren Säulen autokratischer Stabilität (Kooptation und Repression) anschlussfähiger an alle drei Liberalismus-Spielarten, da Legitimation auf unterschiedliche Weise generiert werden kann.[40]

---

40 Zum einen auf der Output-Ebene, etwa durch wirtschaftliche oder militärische Erfolge, oder aber auf der Input-Ebene, beispielsweise durch das Fördern eines Personenkults um den autokratischen Führer, oder aber einer allgemein nationalistisch-patriotischen Legitimierung der Regierung.

Das oberste Ziel autokratischer Regime ist die Sicherung der eigenen Stellung an der Spitze des defizitären bzw. verkürzten Transmissionsriemens im politischen Prozess. Da hierfür der Säule der Legitimation eine immer größere Bedeutung zugeschrieben wird, eignet sich eine solche Regimetypen-Klassifizierung auch besonders für die liberal geprägte Erfassung des Einflusses unterschiedlicher Legitimations- und somit Interessensdurchsetzungsstrategien nach innen und außen. Die Anwendung der gröberen Unterscheidung von Geddes (1999) würde vor allem auf republikanischer und ideeller Ebene zu viele bedeutsame Unterschiede autokratischer Subtypen sowie deren konditionierenden Einfluss der gesellschaftlichen Präferenzkonstellationen nicht erfassen.

Zur Unterscheidung demokratischer Subtypen wird zwischen liberalen und illiberalen Demokratien unterschieden, bei Letzteren liegt der Fokus jedoch auf der populistisch geprägten Variante. Während erstere sich verpflichten, ihre liberalen Norm- und Wertvorstellungen auch auf die tägliche Arbeit in den demokratischen Institutionen zu übertragen, besonders im Hinblick auf den Aspekt der Rechtsstaatlichkeit, unterhöhlen letztere die ursprünglich liberalen demokratischen Institutionen durch deren gesetzlich gedeckte Modifizierung.[41] Liberale Demokratien unterscheiden sich somit von ihrer illiberalen Variante insofern, als sie demokratische Institutionen, Regeln und Prinzipien nicht regelmäßig zu ihren Gunsten ausnutzen und die republikanische Ebene somit die liberal-demokratischen Identitäten des Landes weitgehend widerspiegelt. Illiberale Demokratien weisen dagegen Defizite in einem Teilbereich oder mehreren Teilbereichen des Modells der sog. »*Embedded Democracy*« auf (Merkel 2004).[42] Hierzu kann es, wie im Falle Ungarns unter Viktor Orban, kommen, wenn eine demokratische Regierung zunehmend illiberale Präferenzen entwickelt und demokratische Institutionen und Prinzipien für deren Durchsetzung politisch ausnutzt. Dies erschwert GegnerInnen der illiberalen Regierungshaltung, legitime politische Forderungen stellen und durchsetzen zu können, da deren Herrschaftszugang durch die entsprechenden rechtlichen Anpassungen signifikant beschränkt wurde. In einem solchen Falle führt ein (oftmals populistisch geprägter) Interessenwandel einer demokratischen Regierung dazu, dass diese ihre eigenen Interessen über die demokratische Verfasstheit der politischen Institutionen stellt und in der Folge die Interdependenzbeziehung zu den übrigen domestischen AkteurInnen stärker zu ihren Gunsten modifizieren kann.

Zusammenfassend zeichnen sich liberale Demokratien somit durch schwächere Interessensdurchsetzungschancen gegenüber domestischen AkteurInnen des gesellschaftlichen Spektrums aus. Anhand der gesellschaftlichen Präferenzen lässt sich dies jedoch damit erklären, dass für liberale Demokratien die eigenen Interessen stärker mit denen der breiten, an der Herrschaft zumindest partiell beteiligten Bevölkerung korrespondieren und die hierdurch eingeschränkte politische Autonomie zugunsten

41 In ihrem Buch »*Wie Demokratien sterben*« beschreiben Levitsky and Ziblatt 2018 verschiedene Mechanismen, die zur gewaltfreien Aushöhlung demokratischer Institutionen und Prinzipien seitens demokratischer EntscheiderInnen zur Anwendung gebracht werden können. Beispiele wären die politisch motivierte Besetzung bedeutsamer RichterInnenämter, oder auch die ideelle Untergrabung der Legitimität der traditionellen Medienlandschaft.

42 Diese sind: Bürgerliche Rechte, politische Freiheiten, horizontale Verantwortlichkeiten, effektive Regierungsgewalt sowie die zentrale Ebene des Wahlregimes.

der demokratischen und rechtsstaatlichen Integrität politischer Institutionen bewusst in Kauf genommen wird. In illiberalen Demokratien entwickeln politische EntscheiderInnen dagegen entsprechend dem ausgrenzenden Legitimationsansatz zunehmend Interessen, die den Interessen der breiten Bevölkerung entgegenstehen. Ein weiteres Charakteristikum illiberaler Demokratien kann zudem die zunehmende Erosion der Akzeptanz des Wahlergebnisses seitens der VerliererInnen sein, indem diese von Wahlbetrug und Fälschung sprechen und ihre AnhängerInnenschaft zu Protesten aufrufen. Der ›Sturm auf das Kapitol‹ in den USA am 6. Januar 2021 war hierfür ein prägnantes Beispiel (Shafy 2022).

Bei der Entstehung illiberaler Tendenzen in etablierten Demokratien können institutionelle Merkmale auf republikanischer Ebene eine besondere Rolle spielen. So geht der Liberalismus davon aus, dass Mehrheitsdemokratien grundlegend unkooperativere Strategien nach innen (und außen) verfolgen und in Folge wechselnder Mehrheiten gleichzeitig unzuverlässigere VerhandlungspartnerInnen auf domestischer (und externer) Ebene darstellen (Schimmelfennig 2013, S. 150). Durch das ›The-Winner-takes-it-all‹-Prinzip ist der Herrschaftszugang in solchen Systemen stärker auf die regierende Partei beschränkt, vor allem in Zweiparteiensystemen wie den USA (Meyer 2009, S. 96). Eine bereits im Wahlkampf stärker ausgeprägte Polarisierung zwischen den Lagern kann sich in der Folge vor allem dann auch auf republikanischer Ebene in illiberalen Tendenzen niederschlagen, sofern der/die KandidatIn einer populistischen Partei gewinnt. Populismus wird oftmals mit Ressentiments gegenüber bestehenden politischen Institutionen verbunden. Somit können populistische Regierungen speziell in Mehrheitsdemokratien diese in der Folge eines Wahlsieges effektiver schwächen und gleichzeitig deren liberalen Kern aushöhlen. Interessant ist hierbei jedoch, dass diese Einschränkung demokratischer Institutionen auf republikanischer Ebene von Populisten wie Donald Trump oftmals mit dem Argument vollzogen wird, dass hierdurch die Stimme des Volkes gegenüber dem Establishment durchgesetzt (Mudde 2004, S. 546), in liberaler Terminologie somit der Transmissionsriemen voll zur Entfaltung gebracht würde. Dies geschieht jedoch de facto durch die Schwächung demokratisch konstituierter Institutionen auf republikanischer und ideeller Ebene, wodurch es schlussendlich zu einer Kompromittierung des Transmissionsriemens und zu einer noch stärkeren Zentralisierung des Herrschaftszuganges unter der Ägide der Regierung und ihrer AnhängerInnen kommt. Im Gegensatz dazu sind Konsensdemokratien mit ihren korporatistischen Interessensgruppierungen stärker auf »*compromise and concertation*« (Lijphart 2012, S. 3) ausgerichtet. Die Macht ist bei diesen auf mehr politische AkteurInnen aus allen drei politischen Gewalten aufgeteilt. Zudem erfordert das Verhältniswahlsystem eine größere Kooperation zwischen den AkteurInnen eines Mehrparteiensystems, auch über die nächste Wahl hinaus. Die Durchsetzung populistischer Präferenzen und die Aufweichung demokratischer Institutionen sind in solchen Systemen somit aufgrund des dezentraleren Herrschaftszugangs politischer AkteurInnen schwerer durchzusetzen als in Mehrheitsdemokratien.[43]

43 Von diesem Grundsatz gibt es jedoch auch Abweichungen: So können auch bei Verhältniswahlen rechtspopulistische Parteien zusammen die Mehrheit gewinnen und in der Folge trotz der Notwendigkeit einer Koalitionsbildung ihre illiberalen Präferenzen sukzessive umsetzen, so gesche-

4.4.6 Die nationale Cyberakteursumwelt

Für die Operationalisierung der KV wird für beide Regimetypen ein Mix aus quantitativen und qualitativen Indikatoren herangezogen:

1. Staatliche/behördliche und privatwirtschaftliche Ebene

Der ›National Cyber Power Index‹ (NCPI) des Belfer Center aus Harvard sieht ein mehrdimensionales Bewertungsraster für staatliche Intentionen und staatliche Kapazitäten vor. Aus Sicht der offensiven Cyberproxynutzung werden für letztere primär die Aspekte ›Disabling Adversary Infrastructure (Offense)‹, ›Intelligence-Collection‹ und ›Commercial Gain‹ als relevant erachtet. Die teilweise überlappenden Teilindikatoren (linke Spalte, Tabelle 8) sowie deren Operationalisierungen (Ausprägungen in Tabelle 8) werden für die Bewertung der KV auf autokratischer Seite herangezogen, da diese hierdurch sowohl auf der staatlichen/behördlichen als auch auf der privatwirtschaftlichen Ebene möglich wird. Letztere ist besonders für IT-Unternehmen als demokratische Cyberproxys bedeutsam.

2. Die zivilgesellschaftliche Ebene: HacktivistInnen, UniversitätsabsolventInnen etc.

Auch zivilgesellschaftliche AkteurInnen können als Proxys fungieren. Darunter gefasst werden Personen mit entsprechenden technischen Fähigkeiten, die sie im Rahmen politischer, kommerzieller, akademischer oder krimineller Institutionen/Organisationen eingesetzt haben. Dies könnten HacktivistInnen, patriotische HackerInnen, aber auch UniversitätsabsolventInnen technischer Studiengänge der jeweiligen Länder sein. Im Rahmen der Analyse der KV wird somit an dieser Stelle (in Abwesenheit passender quantitativer Indizes über einen hinreichend großen Teil des Untersuchungszeitraumes) in erster Linie auf entsprechende Primär- und Sekundärquellen verwiesen, die die Existenz und das Ausmaß entsprechender AkteurInnen für die jeweilige Autokratie aufzeigen.

3. Die Ebene der Cyberkriminalität

Zuletzt stellt besonders der nationale Cyberkriminalitätssektor einen potenziellen Ressourcen-Pool für autokratische Cyberproxys dar. Dabei kann es sich um zunehmend im Cyberspace agierende Kriminelle handeln oder aber um genuine Cyberkriminelle, die ausschließlich im Cyberspace aktiv sind. Wie im Falle der zivilgesellschaftlichen Ebene wird zu deren Analyse auf Primär- und Sekundärquellen zurückgegriffen, die das Ausmaß und die Art der jeweiligen nationalen Cyberkriminalitätslandschaft erfassen.

Generell gilt, dass materielle sowie immaterielle Ressourcen vor allem staatlicher, aber auch nichtstaatlicher AkteurInnen aufgrund der im Vergleich zu konventionellen

hen etwa in Ungarn seit 2010 (Filippov 2021). In anderen europäischen Ländern, z.B. Deutschland, verhinderte dies bislang die Haltung etablierter konservativer Parteien, eine Regierungsbildung mit rechtsgesinnten Parteien wie der AfD von vornherein auszuschließen.

Machtdomänen wesentlich stärker auf Geheimhaltung basierenden Dynamik im Cyberspace weniger offensichtlich sind (Schulze 2019, S. 26). Daher ist für eine annähernde Bewertung der hier vorgeschlagene Mix aus quantitativen sowie qualitativen Quellen unterschiedlicher AkteurInnen erforderlich, wie er auch im Rahmen des NCPI zur Anwendung kommt (Voo et al. 2020).

Tabelle 8: Operationalisierung der KV

NCPI-Teilindikatoren* *(staatliche Ziele)*	Operationalisierung
Cyber-Military-Doctrine *(Offense)*	Vorhanden? Wenn ja, seit wann? (*Quellen: Webseiten der jeweiligen Regierungen/Ministerien*)
Cyber-Military-Staffing/National Cyber-Command *(Offense)*	Vorhanden? Wenn ja, seit wann? (*Quellen: Webseiten der jeweiligen Regierungen/Ministerien*)
Global Top-Technology-/Cybersecurity-Firms *(Offense, Commercial Gain, Intelligence)*	Vorhanden? Wenn ja, seit wann? (*Quellen: Cybercrime Magazin, Forbes?*)
High-Tech-Exports *(Offense, Commercial Gain, Intelligence)*	Vorhanden? Wenn ja, seit wann? (*Quellen: World Bank*)

Die Tabelle basiert auf Voo et al. 2020.
* Der Teilindikator ›Existence of Private Sector Surveillance-Technology‹ wurde nicht noch einmal gesondert übernommen, da er deutliche Überschneidungen mit dem ebenfalls enthaltenen Indikator ›High-Tech-Exports‹ aufweist. Gleiches gilt für den Indikator ›Skilled Employees in the Technology-Industry‹ bezüglich des gelisteten Indikators ›Global Top-Technology-/Cybersecurity-Firms‹.

4.4.7 Das allgemeine Konfliktniveau

Für die Operationalisierung des intervenierenden Einflusses gewaltfreier und/oder gewaltsamer Konfliktdynamiken auf der konventionellen Ebene wird der bereits im HD-CY.CON angelegte Nexus zur konventionellen Konfliktforschung des HIIK genutzt. Wie bereits beschrieben, wird in Bezug auf Cybervorfälle nicht nur (sofern plausibel) der angenommene Cyberkonfliktgegenstand kodiert, sondern im Falle eines hiermit verbundenen konventionellen Konfliktes der betroffenen Dyade deren äquivalente Konfliktgegenstände. Darüber hinaus kann die Intensität des Cybervorfalls mit Werten von eins bis fünf zu dessen potenzieller HIIK-Konfliktintensität in Beziehung gesetzt werden.

Neben diesen quantitativen Indikatoren werden qualitative Quellen bezüglich der jeweiligen Konfliktdyaden analysiert, um den Einfluss der Konfliktereignisse auf der konventionellen Ebene im Sinne der aufgestellten Hypothesen testen zu können.[44]

4.5 Auswahl der Leitfragen

Die Auswahl der Leitfragen orientiert sich am liberalen Erklärungsmodell für die Verwendung von Proxys in Cyberkonflikten sowie der Struktur der ausgewählten Fälle. Aus den eingangs formulierten Gesamtforschungsfragen der Arbeit *(»Welche Arten von Proxys im Cyberspace nutzen Autokratien und Demokratien trotz eigener, technischer Kapazitäten? Welche Funktionen übernehmen diese und unter welchen Bedingungen?«)*, ergeben sich folgende, übergeordnete Leitfragen für beide Regimetypen, die die jeweiligen Fallstudien strukturieren:

- Welche Ausprägungen nehmen die beiden AVs in den jeweiligen Fällen an?
- Welchen Einfluss hatte die UV im Zusammenspiel mit den IVs und der KV auf die jeweilige(n) Ausprägung(en) der beiden AVs im betreffenden Fall und lassen sich hierüber Varianzen zwischen den Fällen erklären?
- Welche Befunde der Fallstudien konterkarieren die aufgestellten Hypothesen über die jeweiligen Wirkweisen der Variablen?

Für die Untersuchung autokratischer Cyberproxy-Nutzung bedeutet dies im Hinblick auf die beiden **AVs** folgende Untersuchungsfragen, die implizit beantwortet werden:

- Welche Funktion(en) im Sinne der prävalenten Incident-Types können für den jeweiligen Fall als vorherrschend bezeichnet werden? (AV I)
- Durch welche technischen und zielspezifischen Charakteristika zeichnete sich die Mehrheit der Angriffe aus?
- Welche Durchschnittsintensität bzw. Intensität in Abhängigkeit von der jeweiligen Incident-Type-Klasse liegt für den jeweiligen Fall vor? (AV I)
- Wie lassen sich die am häufigsten/stärksten genutzten Proxys für den jeweiligen Fall hinsichtlich ihrer Art und institutionellen Anbindung charakterisieren? (AV II)
- Lassen sich ›Within-Case‹-Varianzen feststellen? (AV I und AV II)

Für die demokratische Cyberproxy-Nutzung ergeben sich folgende Forschungsfragen zur Analyse der AVs:

- Welche Art von AkteurInnen attribuierte die Mehrzahl der jeweiligen Angriffe? Politische und/oder private AkteurInnen? (AV II)

44 Da das HIIK für manche Konfliktdyaden, wie etwa Iran vs. Saudi-Arabien im Jahr 2015, aus nicht ersichtlichen Gründen zeitweilig keine Kodierungen bereithält, müssen diese zusätzlichen Quellen analysiert werden.

- Welche Art von Zuschreibung wurde vorgenommen? (Blurred[45] vs. True Attribution?) (AV I)
- Wie gestaltete sich die zeitliche Abfolge der getätigten Attributionen (politische vs. technische) in den jeweiligen Fällen?
- Bezog sich die politische Zuschreibung (falls vorhanden) in irgendeiner Weise auf den IT-Sektor und seine Arbeit?
- Gibt es Hinweise oder Belege für eine tatsächliche Zusammenarbeit von Regierungsstellen sowie IT-Unternehmen im Vorfeld von Zuschreibungen?
- Sind personelle Verbindungen zwischen den attribuierenden IT-Firmen sowie der jeweiligen Regierung bekannt?

Um die Ausprägung sowie Wirkweise von UV, IV und KV im jeweiligen Fall bewerten zu können, werden für beide Regimetypen folgende Forschungsfragen implizit beantwortet:

UV:

- Welche domestischen AkteurInnen können für die jeweils zu erklärende Cyberproxy-Nutzung als besonders relevant erachtet werden? (Identifizierung der zentralen Winning Coalitions/Interessensgruppen mit Bezügen zur republikanischen Ebene)
- Wie waren deren Präferenzen auf ideeller und wirtschaftlicher Ebene ausgestaltet bzw. wie führte deren Ausgestaltung zur für die Proxy-Nutzung maßgeblichen Präferenzkonfliktivität gegenüber dem attribuierten Angreifer?
- Welchen Einfluss nahm die republikanische Ebene auf die Interessensdurchsetzung besagter AkteurInnen?
- Auf welche Weise konstituierte die republikanische Ebene selbst die für die Proxy-Nutzung maßgeblichen Vulnerabilitätsasymmetrien nach innen oder außen?

IV:

- Welchen Einfluss hatte das jeweilige allgemeine Konfliktniveau auf die Präferenzkonstellation auf domestischer Ebene?
- Inwiefern nahm das allgemeine Konfliktniveau somit einen direkten Einfluss auf die wahrgenommenen, eigenen oder fremden Vulnerabilitätsasymmetrien, die es durch die Proxy-Nutzung zu manipulieren galt?

KV:
Durch die Fallauswahl ergibt sich für die KV bereits notwendigerweise eine positive Ausprägung im Sinne des Vorhandenseins staatlicher sowie nichtstaatlicher AkteurInnen

45 Als ›Blurred Attributions‹ werden in der Folge solche Zuschreibungen bezeichnet, die keinen spezifischen Akteur als Verantwortlichen benannt haben und beispielsweise nur von ›TäterInnen aus dem Land X‹ oder ›vermutlich staatlich gesponserten AkteurInnen‹ ohne Nennung eines konkreten Landes sprechen.

mit entsprechenden Fähigkeiten im Cyberspace, weshalb im Rahmen der empirischen Untersuchung für deren Analyse folgende Frage im Mittelpunkt steht:

- Inwiefern konditionierte die KV durch ihre Ausprägung die jeweilige Cyberproxy-Nutzung autokratischer oder demokratischer Staaten, insbesondere im Hinblick auf die AV II?

5. Die empirische Cyberkonfliktlandschaft von 2000–2019: Der HD-CY.CON-Datensatz

Der HD-CY.CON erfasste für einen bestimmten Zeitraum neben englisch- und deutschsprachigen auch chinesisch- und russischsprachige Quellen. Warum diese multilinguale Kodierpraxis jedoch nicht auf den gesamten Untersuchungszeitraum ausgeweitet wurde und welche Implikationen dies für den Untersuchungsgegenstand staatlicher Attributionspraktiken haben könnte, wird nachfolgend erläutert. Daran anschließend erfolgen die Beschreibung und die Analyse des Gesamtdatensatzes hinsichtlich der autokratischen sowie demokratischen Fallauswahl für die empirische Analyse.

5.1 Cyberkonflikte und deren Darstellungen in russisch- und chinesischsprachigen Quellen

Die Kodierung von Cyberkonflikten entsprechend der Vorgehensweise im Rahmen des HD-CY.CON speist sich in erster Linie aus öffentlich zugänglichen Quellen: Regierungsseiten, Online-Auftritte von Zeitungen, wissenschaftliche Online-Quellen sowie Berichte von IT-Firmen. Das Projekt von vornherein auf ausschließlich westliche Quellen bzw. deren Sprachen (englisch und deutsch) zu beschränken, hätte somit zu einer verzerrten Darstellung der öffentlich verfügbaren Informationslage führen können. Dem zugrunde liegt die Annahme, dass die Berichterstattung bzw. die Informationen der jeweiligen AkteurInnen auch durch deren soziokulturellen Hintergrund und somit durch ihre Sprache beeinflusst werden könnten. Für Cyberoperationen ist hierbei der Aspekt der Attribution zentral: Nehmen russisch- oder chinesischsprachige Quellen/AkteurInnen regelmäßig sich von ihren englischsprachigen Pendants unterscheidende Attributionen vor? Russisch und Chinesisch qualifizierten sich als Vergleichssprachen aus mehreren Gründen:

1. Sowohl China als auch Russland gelten als führende Staaten im Bereich des offensiven Cyberkonfliktgeschehens. Sie stellen somit eine Art Gegenpol zur durch die USA dominierten westlichen ›Cybersphäre‹ dar. Ihre stärkere Involvierung lässt ihre Be-

richterstattung über das eigene, aber auch fremde Konfliktverhalten plausibel und untersuchungswürdig erscheinen. Voraussetzung hierfür ist die Annahme, dass die beiden Sprachräume durch die autokratische Verfasstheit der jeweiligen Länder bezüglich Form und Inhalt entscheidend beeinflusst werden. Worüber wird berichtet? Welche Informationen werden regelmäßig veröffentlicht? Welche AkteurInnen sind hierfür hauptsächlich verantwortlich? Lassen sich Muster hinsichtlich inhaltlicher Attributionspraktiken feststellen bzw. widersprechen diese regelmäßig jenen westlicher Länder?

2. Aufgrund des technologischen Entwicklungsstands und ausgeprägten Anspruchsdenkens Russlands und Chinas im Digitalsektor kann auch von einer größeren Salienz der Thematik innerhalb dieser beiden Kulturräume bzw. von sophistizierteren, eigenen technischen (und politischen) Attributionskapazitäten ausgegangen werden. Zudem stellten beide Länder mit ihrer Prägung des Begriffs der ›Informationssicherheit‹ dem westlich geprägten Konzept der ›Cybersicherheit‹ ein Pendant gegenüber und können als autokratische Normentrepreneure gewertet werden (Austin 2016). Diesen Ansatz propagierten sie im Rahmen regionaler autokratisch dominierter Organisationen wie der Shanghaier Organisation für Zusammenarbeit (SOZ),[1] aber auch auf UN-Ebene in Form verschiedener Resolutionen.[2] Ziel war und ist es dabei, staatliche Kontroll- und Interventionsmöglichkeiten und -rechte mit dem Verweis auf deren Notwendigkeit zur Bekämpfung von Cyberkriminalität und Terrorismus gegenüber der eigenen Bevölkerung zu stärken.
3. Während Russland ein im Vergleich teilweise offenes Internet aufweist, bedingt zu einem Großteil durch die stärkere wirtschaftliche Integration im und Abhängigkeit vom globalen, digitalen Ökosystem,[3] zeichnet sich das chinesische Internet als ein de facto durch die ›Great Firewall of China‹ national abgeschottetes Intranet aus (Roth 2019). Somit können durch die Analyse russischer und chinesischer Quellen potenzielle Unterschiede nicht nur zum westlichen Kulturraum, sondern auch zueinander untersucht werden.

Nachdem für die Jahre 2013 bis 2016 chinesisch- und russischsprachige Quellen sowohl unabhängig voneinander als auch im Vergleich zu ihrem jeweiligen englischsprachigen Gegenpart in ca. 50 Fällen kodiert wurden, wurde folgendes Bild deutlich:

---

1 Bereits 2009 schlossen die Staaten der SOZ ein Abkommen über »*Cooperation in the Field of International Information Security*« Shanghai Cooperation Organization 2009.

2 Hierbei handelte es sich um zwei Resolutionen der UN aus 2018, die beide Initiativen Russlands darstellten: Die erste Resolution A/RES/73/187 trug dabei den vielsagenden Titel »*Countering the use of information and communications technologies for criminal purposes*«. Bei der zweiten Resolution A/RES/73/27 wurde dagegen die Gründung einer Open-Ended-Working-Group für das Vorantreiben von Normen im Cyberspace beschlossen. Die USA sowie deren Verbündete votierten jeweils dagegen, da man diese Bestrebungen als Versuche Russlands und weiterer Autokratien ansah, deren nationale Repressions- und Zensurmaßnahmen international legitimieren zu lassen (Peters 2019).

3 Auch wenn sich Russland vor allem mit dem im November 2019 in Kraft getretenen »*Sovereign Internet Law*« dem Modell Chinas immer stärker annähert (Epifanova 2020), klaffte hinsichtlich der Geschlossenheit der jeweilig nationalen Digitalinfrastrukturen im Untersuchungszeitraum 2013–2016 jedoch noch eine weitaus größere Lücke zwischen den beiden Ländern.

1. Es konnten keine regelmäßigen Trends oder Muster für die beiden nicht westlichen Staaten im Hinblick auf eine differenzierte inhaltliche Attribution im Gegensatz zu den entsprechenden englischen Quellen ausgemacht werden. Zudem wurden nahezu sämtliche recherchierten Fälle ebenso von westlichen Quellen abgedeckt. Somit kann die These, dass beispielsweise russische Quellen dazu neigen, regelmäßig von der westlichen Attributionspraxis abzuweichen, nicht bestätigt werden. Gleiches gilt für die untersuchten chinesischsprachigen Quellen.
2. Während für russischsprachige Quellen eine gewisse institutionelle Vielfalt ausgemacht werden konnte und insgesamt häufiger über konkrete Cybervorfälle berichtet wurde, zeichnete sich für chinesische Quellen ein differenziertes Bild: Die Unterscheidung zwischen nichtstaatlichen und staatlichen AkteurInnen ist zunächst weitaus schwieriger als im Falle Russlands. Hiervon unabhängig konnte für China jedoch insgesamt ein geringes Maß an Berichterstattung über Cyberoperationen im In- und Ausland festgestellt werden. Auch wenn in manchen Fällen staatliche Medien wie China News oder Xinhua über Cyberoperationen berichteten und diese Informationen dann auch vereinzelt seitens großer chinesischer Internetunternehmen wie Sohu.com wortgleich übernommen wurden, war diese Praxis doch eher die Ausnahme. Die Berichte waren meist oberflächlich, ohne konkrete Details der Vorfälle zu diskutieren.
3. Im Gegensatz dazu berichteten manche Privatunternehmen auf ihren Webseiten häufiger über Cyberoperationen. Ein Beispiel hierfür ist die Seite chinabyte.com比特网, die zur Tianji-Media Gruppe gehört (TMG 2014). Auch wenn somit von einer gewissen IT-Berichterstattung außerhalb staatlicher Medienkanäle gesprochen werden kann, operiert diese doch stets innerhalb der Rahmenbedingungen der umfangreichen Kontroll- und Zensurapparate. Auf inhaltlicher Ebene lässt sich feststellen, dass sich die recherchierten chinesischen Quellen vornehmlich auf Cybervorfälle im Ausland bezogen und innerchinesische Cyberoperationen somit in gewisser Weise zensierten. Die Informationshoheit liegt auch im Cyberspace bei der Kommunistischen Partei, die kein Interesse daran haben dürfte, eigene Verwundbarkeiten vor der eigenen Bevölkerung als Audience zu diskutieren. Daher konzentrierten sich die wenigen IT-Berichte auf das Ausland und übernahmen zeitweilig Informationen westlicher Quellen wörtlich in das Chinesische. Somit überträgt sich die Informationshoheit der Kommunistischen Partei Chinas auch auf den Bereich der Cyberoperationen seitens/in China. Anders als erwartet, wird diese jedoch nicht zu Propagandazwecken missbraucht.[4]
4. Im Falle russischsprachiger Quellen konnte deren Analyse zumindest etwas häufiger Politisierungen einzelner Falle nachweisen, als es über eine ausschließliche Kodierung westlicher Quellen möglich gewesen wäre. Dies zeigt, dass der innerrussische Diskurs vor allem inländische Cyberoperationen häufiger und umfassender

4 Gegenüber der internationalen Audience stellen Regierungsoffizielle die VR jedoch immer wieder als Opfer zahlreicher Cyberoperationen dar, konfrontiert mit Vorwürfen eigener Operationen. Diese »Quasi-Attributionen« sind jedoch genereller Natur und verweisen auf keine konkreten Vorfälle und liefern auch keine weiterführenden Informationen hierüber.

adressiert als im Falle Chinas. Politisierungen von Cyberoperationen durch chinesische PolitikerInnen konnten nicht festgestellt werden. Der chinesische Staat bzw. die Kommunistische Partei äußerten sich, wenn, dann lediglich zumeist ablehnend gegenüber ausländischen Schuldzuweisungen bezüglich Cyberangriffen, thematisierten diese jedoch regelmäßig nicht selbst. Dennoch verwiesen Internetquellen der chinesischen ›*IT-Sicherheitscommunity*‹ immer wieder auf Informationen der chinesischen Version der *Global Times* (*huanqiu wang* 环球网), einem Propagandaorgan der Kommunistischen Partei. Deren Artikel enthielten jedoch meist nur oberflächliche Angaben und somit nicht die für eine Kodierung im Rahmen des Datensatzes notwendigen Informationen zu Zielen oder der technischen Vorgehensweise im Rahmen der Operationen.[5]

5. Für China war zudem bemerkenswert, dass sich einzelne Quellen an westlichen Quellen aus dem IT-/Technologie-Sektor bedient und diese teilweise wörtlich übernommen haben.[6] Ferner zitierten chinesische Quellen regelmäßig US-amerikanische Sicherheitsfirmen. Somit lässt sich für die chinesischen Quellen, wenn überhaupt, am ehesten von einer tendenziell US-amerikanisch geprägten Berichterstattung über jedoch im Ausland stattgefundene Cyberoperationen sprechen.

Der vermutete sprachlich-kulturelle Bias konnte somit (zumindest für die untersuchten Jahre) nicht nachgewiesen bzw. eher noch entkräftet werden. Es scheint auf Grundlage der untersuchten Fälle keine Anhaltspunkte für eine regelmäßige ›Attributionsparallelwelt‹ innerhalb der russisch- und chinesischsprachigen Gemeinschaft zu geben. Lediglich eine weitaus geringere Häufigkeit sowie Ausdifferenziertheit hinsichtlich der Berichterstattung in der jeweiligen Nationalsprache konnten nachgewiesen werden. Dieser Umstand lässt sich durch die autokratische Regimelogik erklären: Die der eigenen Bevölkerung zur Verfügung gestellten Informationen unterliegen strikteren Kontrollregeln als etwa englischsprachige Berichte heimischer Firmen, die stärker die internationale Gemeinschaft adressieren. Auch russische oder chinesische IT-Firmen, die technische Berichte im Zuge von Cyberoperationen veröffentlichen, etwa Kaspersky Lab[7],

5 Gleiches gilt für die jährlichen Cyberberichte des »*National Computer Network Emergency Response Technical Team/Coordination Center of China*« (CNCERT), einer offiziell nichtstaatlichen, de facto jedoch mit politischen Institutionen eng zusammenarbeitenden Behörde. Die Berichte waren bislang überwiegend technischer Natur und lieferten nur selten Details etwa über die angegriffenen Ziele, oder auch die vermuteten AngreiferInnen. Weitere Informationen zum CNCERT finden sich unter http://www.cert.org.cn/publish/english/index.html.

6 Ein Beispiel hierfür wäre die chinesische Webseite freebuf.com, die Informationen der US-amerikanischen IT-News-Seite hackread.com oftmals wörtlich in das Chinesische übersetzt.

7 Kaspersky Lab ist neben US-amerikanischen IT-Firmen führender Softwarehersteller weltweit und auch im Bereich der Threat-Analysis Research, der Aufdeckung von Cyberoperationen, ein prominenter Vertreter. Die Debatte, inwiefern – auch aufgrund persönlicher Beziehungen des Mitbegründers Jewgeni Kaspersky zum russischen Präsidenten Putin – die Firma tatsächlich, wie von den USA 2017 behauptet, wissentlich als verlängerter Spionagearm des Kremls angesehen werden sollte, kann an dieser Stelle nicht bewertet werden. Der israelische Geheimdienst war in die Server von Kaspersky Berichten zufolge bereits 2014 eingedrungen und konnte die NSA in der Folge warnen, dass die Antivirensoftware der Firma seitens Russlands offenbar für Spionagezwecke genutzt wurde. Daraufhin erließen die USA ein Verbot von Kaspersky-Produkten in staatlichen Ein-

Group-IB und Positive Technologies auf russischer sowie Qihoo 360 auf chinesischer Seite, veröffentlichen diese in den meisten Fällen auch auf Englisch.

Da keine plausiblen Gründe vorlagen, warum sich diese Beobachtungen nicht aller Wahrscheinlichkeit nach auch auf die übrigen Jahre des Datensatzes übertragen lassen, wurden Recherche und Analyse chinesisch- und russischsprachiger Quellen nach Bearbeitung des Zeitraumes 2013–2016 vorerst eingestellt. Für eine breite, effiziente und transparente Kodierung ist langfristig vor allem die Verwendung englischsprachiger Quellen gerechtfertigt, besonders, da sich aufgrund der Vorreiterrolle westlicher IT-Firmen in den untersuchten Beispielen AkteurInnen nichtwestlicher Länder häufig auf deren Informationen hinsichtlich der Attribution stützten. Zudem ist Englisch gerade im IT-Bereich die gängigste Sprache, unabhängig davon, aus welchem Land der jeweilige Akteur stammt.

Dennoch sollte der Aspekt einer graduell verschobenen Attributionspraxis nicht völlig außer Acht gelassen werden, da er im Falle einer zunehmenden technischen Fragmentierung des Internets an Bedeutung gewinnen könnte. Für die Kodierpraxis im Hinblick auf einen fortlaufend öffentlich einsehbaren Datensatz wurde sie jedoch im Rahmen des Projekts aufgrund der genannten Aspekte als nicht signifikant bewertet.

5.2 Regimetypenspezifische Cyberproxy-Nutzungsmuster im HD-CY.CON

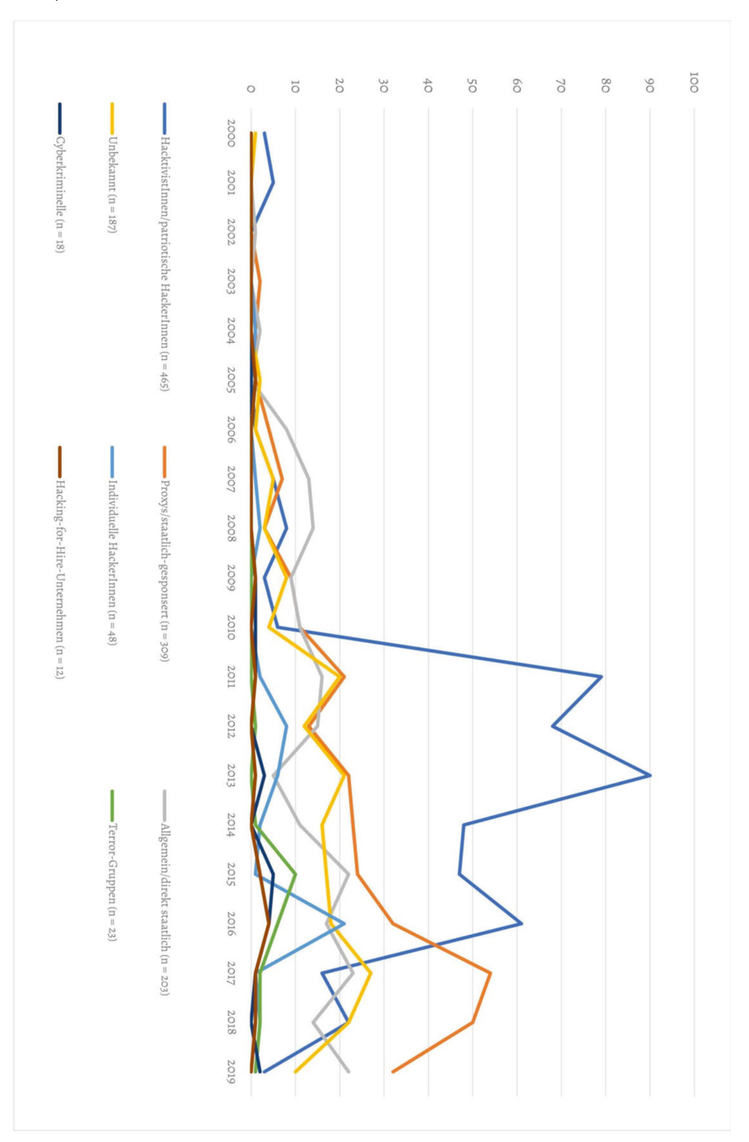
Für eine theoriegeleitete Auswahl der autokratischen und demokratischen Fallbeispiele wird im Folgenden der HD-CY.CON für den Zeitraum von 2000 bis 2019 (Anfangsjahre der jeweiligen Cyberoperation) statistisch beschrieben. Dies ist notwendig, um erstens plausibel begründen zu können, dass sich die aufgestellten Metahypothesen bezüglich der vermuteten prävalenten autokratisch-offensiven und demokratisch-defensiven Cyberproxy-Nutzung auch auf Grundlage der empirischen Daten bekräftigen lassen, und zweitens, um die für das Erkenntnisinteresse der Arbeit sinnvollsten Fälle, hier also Länder, auszuwählen.

Abbildung 10 veranschaulicht die im Datensatz verzeichneten AngreiferInnen-Attributionen zwischen 2000 und 2019. Den größten Anteil nehmen nichtstaatliche AkteurInnen, genauer gesagt die Gruppe der HacktivistInnen/patriotischen HackerInnen, mit 465 Vorfällen ein. Ein deutlicher Anstieg der ihnen zugesprochenen Cyberoperationen ist vor allem ab 2011 zu beobachten. Dies mag im Falle nichtstaatlicher AkteurInnen weniger als für staatliche Cyberoperationen am sog. »*Stuxnet-Effekt*« (Farwell und Rohozinski 2011; Collins und McCombie 2012) nach 2010 und mehr an der Zunahme regionaler Konflikte während des Arabischen Frühlings ab 2011 sowie am ausgeweiteten und intensivierten Aktionsradius des internationalen Hackerkollektivs Anonymous liegen. Jedoch ist die mit den Jahren gestiegene Aufmerksamkeit, die Cyberkonflikte seitens eines immer breiteren Spektrums an staatlichen, privatwirtschaftlichen sowie zivilgesellschaft-

richtungen. Kaspersky selbst bestritt stets jegliche Vorwürfe dieser Art, mit dem Hinweis auf die Zusammenarbeit mit staatlichen Stellen vieler Länder, jedoch stets im Rahmen defensiver Strafverfolgungskooperationen und nicht offensiver Spionagetätigkeiten (Horchert 2017).

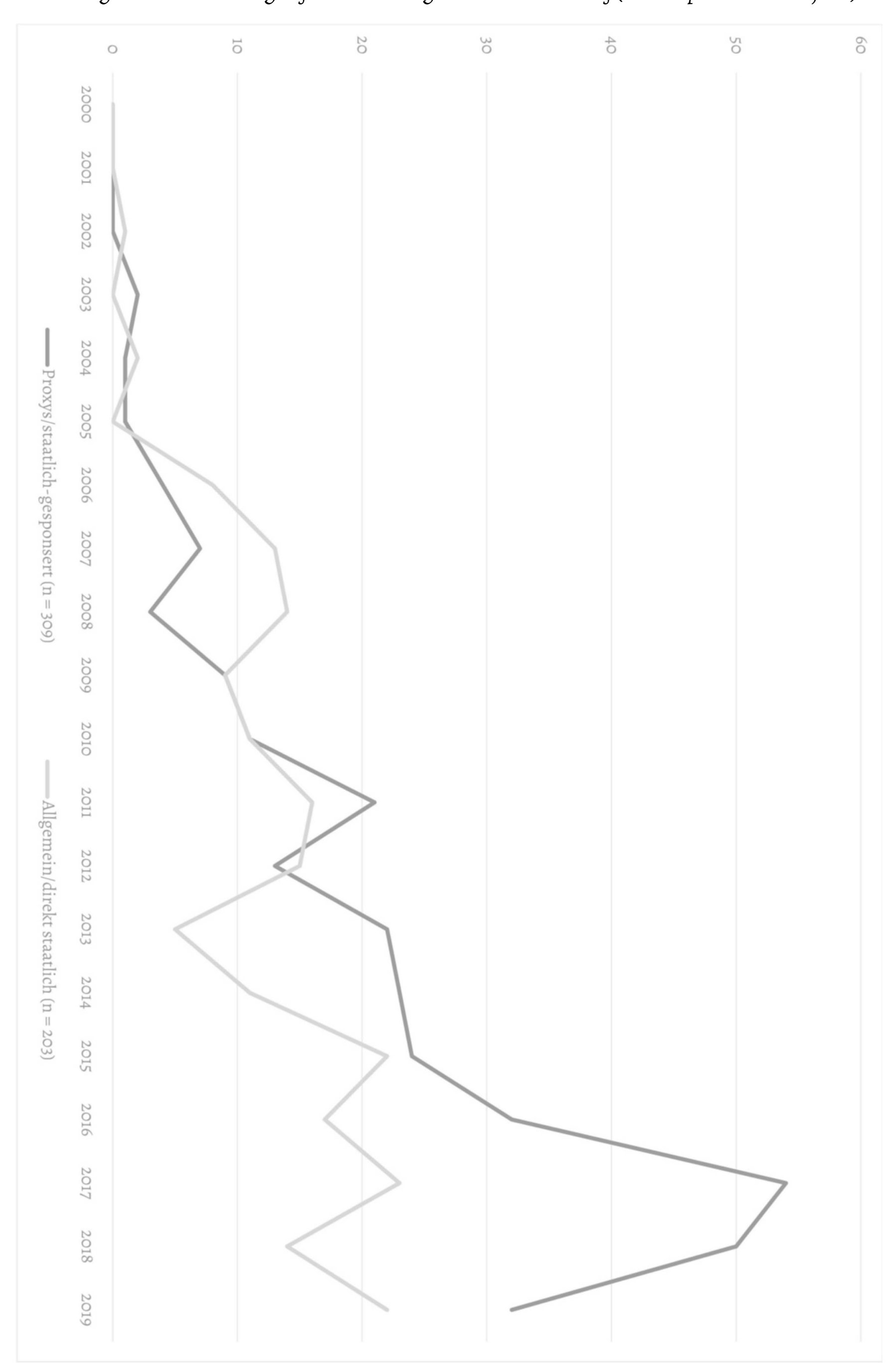
lichen AkteurInnen erfahren haben, als ein zusätzlicher Faktor für die stetig steigenden Fallzahlen nicht von der Hand zu weisen.

Abbildung 10: AngreiferInnen-Attributionen im Zeitverlauf (nach Operationsstartjahr)



(Eigene Darstellung auf Basis des HD-CY.CON)

Abbildung 11: Staatliche AngreiferInnen-Kategorien im Zeitverlauf (nach Operationsstartjahr)



(Eigene Darstellung auf Basis des HD-CY.CON)

Im Falle der Cyberoperationen mit attribuierter staatlicher Involvierung (isoliert dargestellt in Abbildung 11) übertreffen die staatlich gesponserten Proxys zugesprochenen Vorfälle (309) quantitativ die allgemein/direktstaatlich attribuierten Operationen (203). Insgesamt scheinen vor allem die Proxy-Operationen ab 2011 mit zeitweiligen Rückgängen kontinuierlich zuzunehmen, der Anstieg im Datensatz als allgemein/direktstaatlich verzeichneter Operationen fiel dagegen moderater aus.

Für die zuletzt erfassten Jahre 2018 und 2019 ist aufgrund oftmals zeitlich verzögerter Detektions- und Attributionsprozesse eine weitere Zunahme relevanter Cyberoperationen zu erwarten. Je kürzer das betreffende Operationsstartjahr zurückliegt, desto stärker ist mit einem Anwachsen der zu verzeichnenden Zahlen in Zukunft zu rechnen. So ist es wahrscheinlich, dass sich z.B. der in 2018 angedeutete Rückgang verzeichneter Proxy-Operationen nach einiger Zeit aufgrund gestiegener Fallzahlen für das Jahr in einen Anstieg gegenüber 2017 wandeln könnte.

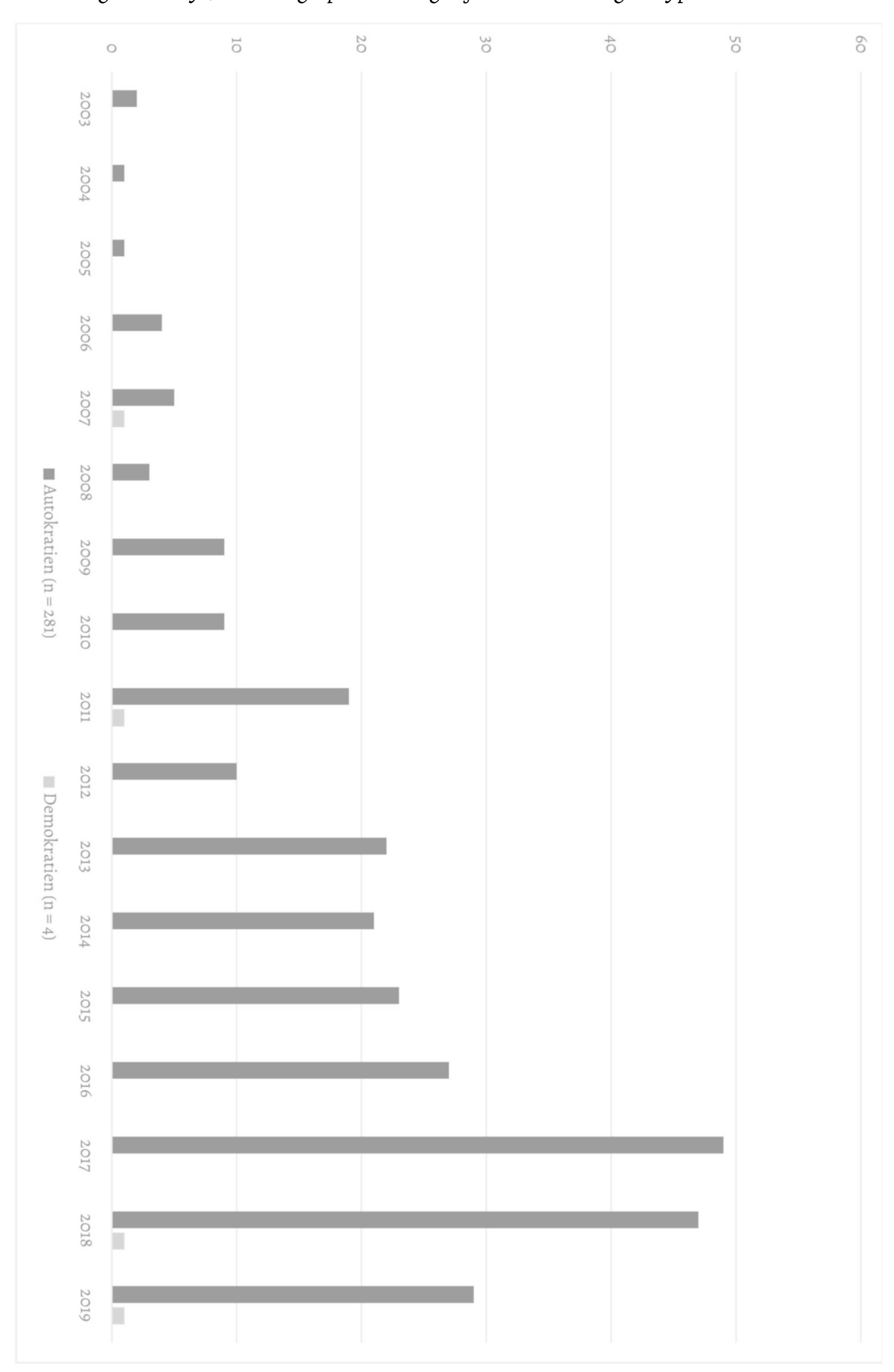
5.2.1 Kennzahlen offensiver Cyberoperationen im HD-CY.CON

Trotz der angesprochenen Teilvorläufigkeit quantitativer Fallzahlen bekräftigt der in Abbildung 12 dargestellte Zusammenhang zwischen staatlich gesponserten Proxy-Attributionen und (im Falle einer vorhandenen Länder-Attribution) dem Regimetyp des vermuteten Auftraggebers die zentrale Annahme der Arbeit, dass vor allem Autokratien offensive StellvertreterInnen im Cyberspace für ihre Zwecke nutzen. So wurden in 281 Fällen autokratische AkteurInnen hinter Proxy-Operationen vermutet, im Gegensatz zu lediglich vier demokratischen Proxy-Attributionen (in allen vier Fällen mit Südkorea als attribuiertem Unterstützerstaat der Gruppe DarkHotel).[8] Die zeitliche Entwicklung autokratischer Proxy-Operationen korrespondiert dabei weitgehend mit der allgemeinen Zunahme attribuierter Proxy-Operationen entsprechend ihrer prozentualen Abdeckung von 90,94 Prozent.

Die durchschnittliche (gewichtete) Intensität aller Proxy-Operationen im Datensatz beträgt für 2000 bis 2019 den Wert 2,28, für allgemein/direktstaatlich attribuierte Vorfälle 2,51, was angesichts des Skalenspektrums einen eher geringfügigen Unterschied darstellt.

8 Neunmal wurde dabei ein Initiator Country kodiert, welches im Operationsstartjahr durch Freedom House als ›Partly Free‹ eingestuft wurde.

Abbildung 12: Proxys/staatlich gesponserte AngreiferInnen nach Regimetyp



(Eigene Darstellung auf Basis des HD-CY.CON)

Im Falle von allgemeinen/direktstaatlichen AngreiferInnen zugesprochenen Cyberoperationen zeigt sich dagegen ein deutlich geringerer Unterschied zwischen den Regimetypen (Abbildung 13): In 123 Fällen waren die attribuierten Staaten autokratisch, in 62 Fällen demokratisch.[9] Das entspricht einem Anteil von 60,59 Prozent für Autokratien und 30,54 Prozent für Demokratien an der Gesamtzahl allgemein/direktstaatlich attribuierter Operationen.[10] Die These vom monadischen ›demokratischen Cyberfrieden‹ kann somit entkräftigt werden. Vielmehr scheint es, dass demokratische Staaten tatsächlich weniger Wert auf die Verschleierung der eigenen Verantwortlichkeit im Falle offensiver Cyberoperationen legen, was einen zentralen Grund für staatliche Proxy-Nutzungen darstellt. Damit wird nicht behauptet, dass demokratische Cyberoperationen nicht auch im Sinne einer zu verhindernden Detektion auf die Verschleierung der Tat an sich ausgerichtet sein können. Der Befund, dass ein Drittel aller allgemein/direktstaatlich attribuierten Cyberoperationen jedoch Demokratien angelastet wurde, spricht aufgrund der oftmals überlegenen technischen Fertigkeiten demokratischer Cybereinheiten, das eigene Handeln verdeckt zu gestalten, für ein zumindest teilweise intendiertes Offenlegen der eigenen Handlung sowie der Urheberschaft. Noch bedeutender kommt jedoch als weiterer Erklärungsstrang für die hohe Zahl an allgemeinen/direktstaatlichen Cyberoperationen demokratischer Staaten hinzu, dass von den 62 Fällen allein 26 der amerikanischen National Security Agency (NSA), teilweise in Kooperation mit dem britischen Government Communications Headquarters (GCHQ), zugesprochen wurden, basierend auf den Enthüllungen des Whistleblowers Edward Snowden. Weder diese auf Geheimhaltung ausgerichteten Operationen noch die amerikanische Urheberschaft sollten an die Öffentlichkeit gelangen. Aufgrund der technologischen Überlegenheit besonders der demokratischen Five-Eyes-Staaten im Überwachungssektor ist somit für diese von einer besonders hohen Dunkelziffer an nicht öffentlich bekannten Cyberoperationen, wohl vor allem Spionage, auszugehen.

Des Weiteren fällt auf, dass die allgemeinen/direktstaatlichen Attributionen gegenüber Autokratien und Demokratien zeitlich invers verschoben sind. Während für demokratische (und vor allem amerikanische) Cyberoperationen der zeitweilige Höhepunkt 2009 respektive 2012 verzeichnet wurde, stieg die Zahl autokratischer Operationen bis zum Jahr 2015 an und blieb auch in der Folge konstant hoch.

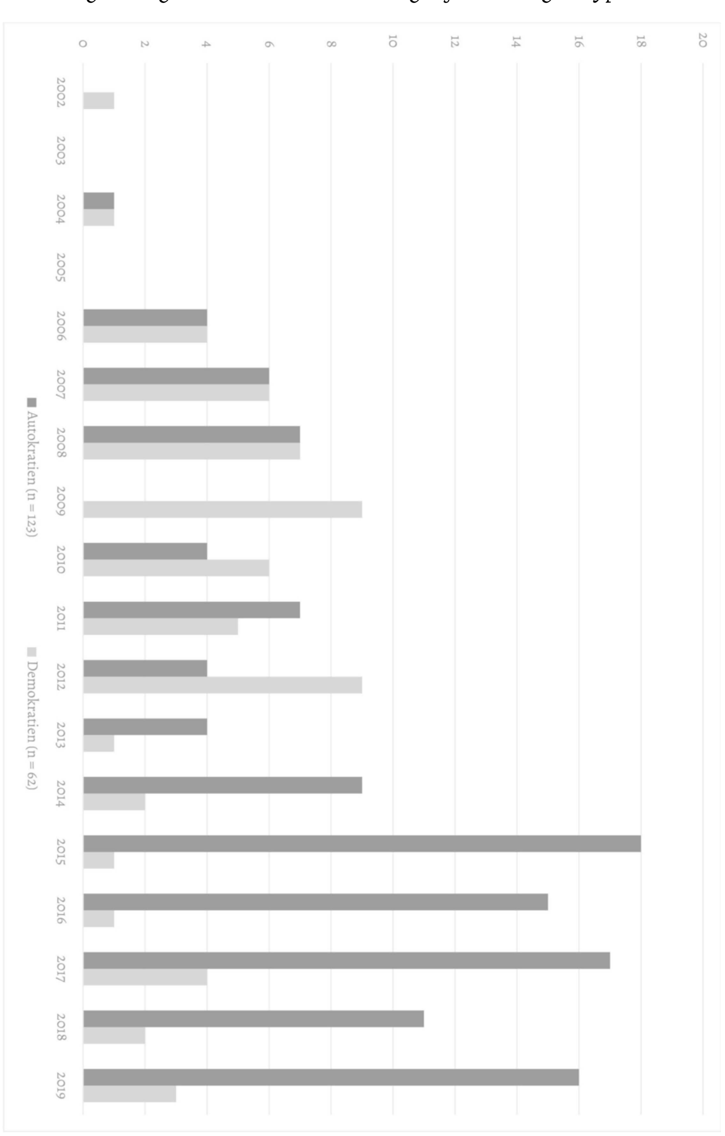
Auch die Annahme der autokratischen Cyberproxy-Operationen gegen primär demokratische Ziele lässt sich durch die Daten des HD-CY.CON weitgehend bekräftigen. So zeigt Abbildung 14, dass ca. 66,55 Prozent aller autokratischen Cyberproxy-Operationen gegen AkteurInnen oder Institutionen in demokratischen Ländern gerichtet waren. Dass jedoch immerhin 35 Proxy-Operationen andere Autokratien betrafen, spricht gegen die Alleingültigkeit des Motivs der Plausible Deniability. Gegenüber anderen Autokratien könnten stattdessen – vor allem im Falle bereits existierender konventioneller Konflikte – primär technische Fähigkeiten/Ressourcen der Proxys eine Rolle gespielt haben,

9 Zehnmal wurde dabei ein Initiator Country kodiert, welches im Operationsstartjahr durch Freedom House als ›Partly Free‹ eingestuft wurde.

10 Der Rest ergibt sich aus Fällen in welchen lediglich die Initiator Category, nicht aber das Land und somit auch nicht der Regime Type kodiert werden konnten.

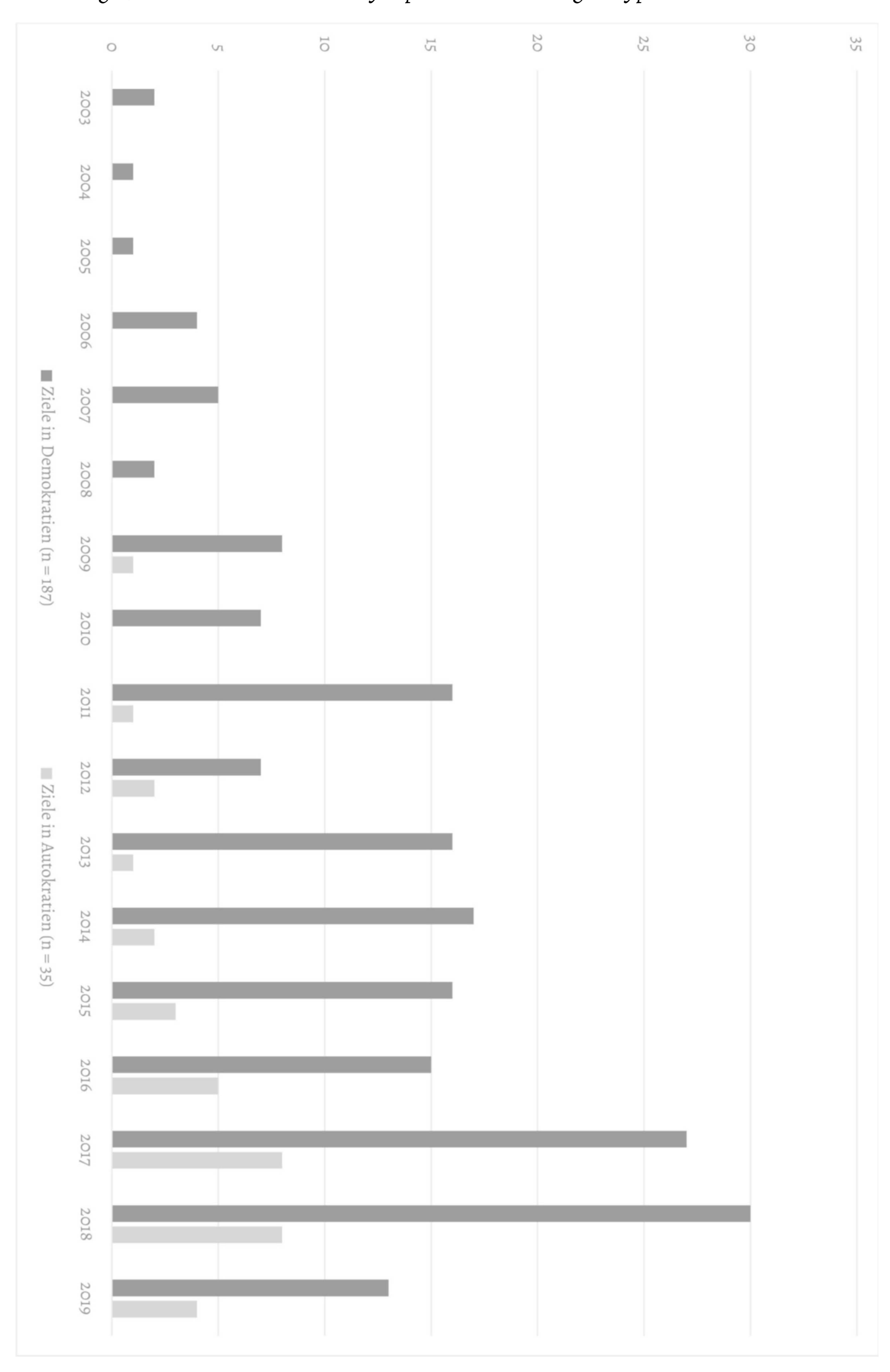
oder aber deren Instrumentalisierung, um eigene staatliche AkteurInnen auf der Cyberebene nicht zu stark zu ermächtigen. Welche der jeweiligen Erklärungsansätze für zwischenautokratische Cyberproxy-Operationen mehr oder weniger Erklärungskraft versprechen, wird Gegenstand der beiden autokratischen Fallstudien sein.

Abbildung 13: Allgemeine/direktstaatliche Angreifer nach Regimetyp



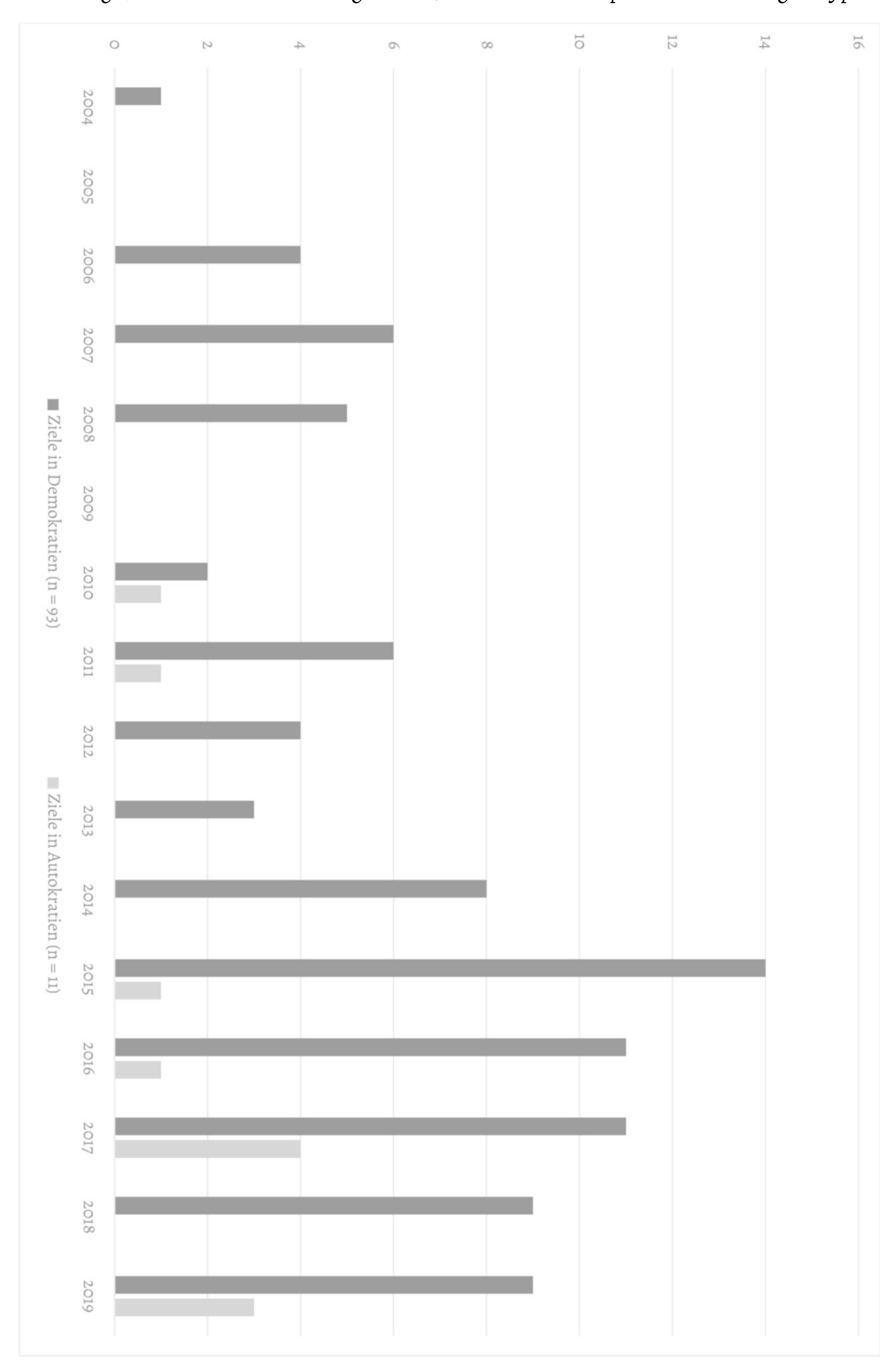
(Eigene Darstellung auf Basis des HD-CY.CON)

Abbildung 14: Ziele autokratischer Proxy-Operationen nach Regimetyp



(Eigene Darstellung auf Basis des HD-CY.CON)

Abbildung 15: Ziele autokratischer allgemeiner/direktstaatlicher Operationen nach Regimetyp



(Eigene Darstellung auf Basis des HD-CY.CON)

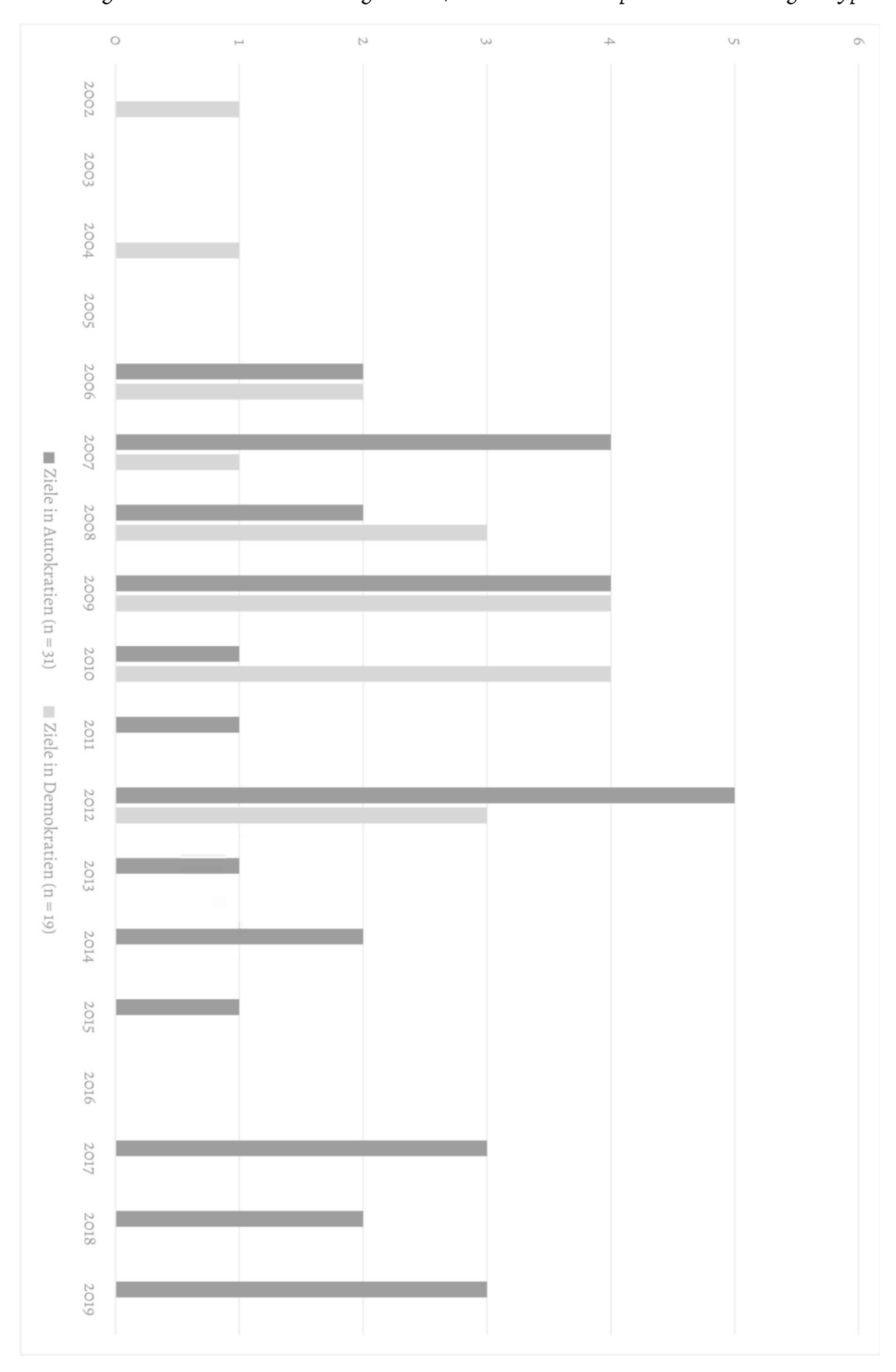
Im Falle allgemeiner/direktstaatlicher Operationen mutmaßlich autokratischer Staaten ist die Verteilung dagegen noch stärker in Richtung demokratischer Ziele ausgestaltet. Lediglich in elf der 123 Fälle waren autokratische AkteurInnen oder Institutionen betroffen (Abbildung 15). Dieser Befund weicht erstmals von den bislang theoretisierten Überlegungen ab. So wäre durchaus ein größerer Anteil autokratischer Ziele unter allgemeinen/direktstaatlichen Cyberoperationen autokratischer Länder zu erwarten gewesen, da zwischen Autokratien u.a. aufgrund ihrer oftmals bereits auf der konventionellen Ebene konfliktiveren Beziehung sowie der militärisch grundlegend ausgeglicheneren Kräfteverhältnisse weniger Anreize für offensive Verschleierung und defensive Attributionszurückhaltung gegeben sein sollten. Dieser Befund wird ebenfalls Teil der nachfolgenden Fallstudien sein. Auf demokratischer Verteidigungsseite wird z.B. untersucht werden, ob sich das Attributionsverhalten über Zeit veränderte und autokratische AkteurInnen ab einem gewissen Zeitpunkt nicht mehr als Proxys, sondern direktstaatlich attribuiert wurden. Dies könnte Teil der Erklärung sein, warum die Zahl an allgemeinen/direktstaatlichen Cyberoperationen autokratischer Länder gegenüber Demokratien im Vergleich zu autokratischen Zielen so hoch ist.

Auch die These vom ›dyadischen, demokratischen Cyberfrieden‹ wird durch Abbildung 16 entkräftet. So waren 19 der 62 demokratischen, allgemeinen/direktstaatlichen Operationen gegen andere Demokratien gerichtet. Dies entspricht einem Anteil von 30,65 Prozent.[11] Demokratien hacken somit nicht nur Autokratien, sondern auch alliierte Staaten mit geteilten normativen Wertvorstellungen. Hacken ist jedoch nicht gleich Hacken: So wurden für rein demokratische Konfliktdyaden keine disruptiven Operationen erfasst, im Gegensatz zu demokratischen Cyberoperationen gegen Ziele in Autokratien, die in fast jedem zweiten Fall disruptiver Natur waren. Da disruptive Cyberoperationen detektiert werden *müssen*, deuten diese Befunde auf eine generell niedrigere Eskalationsaversion demokratischer Staaten gegenüber Autokratien auch im Cyberspace hin. Bedeutsam ist hier jedoch, dass abermals die USA für einen Großteil der disruptiven Cyberoperationen auf autokratische Ziele (zumeist alleinig) verantwortlich waren. Nicht nur im Bereich der auf Geheimhaltung der eigenen Handlung und Verantwortlichkeit ausgerichteten Cyberspionage, sondern auch für sichtbarere, zerstörerische Cyberoperationen bestimmen die USA somit quantitativ sowie qualitativ das demokratische Cyberkonfliktaustragungsmuster im Untersuchungszeitraum.

Wird Cyberspionage als friedliche Handlung betrachtet, könnte dagegen auf Grundlage der Daten die These vom ›dyadischen, demokratischen Cyberfrieden‹ eher bekräftigt werden.

11 Aufgrund der geringen Anzahl demokratischer Proxy-Operationen wird an dieser Stelle auf eine gesonderte Analyse der anvisierten Ziele verzichtet.

Abbildung 16: Ziele demokratischer allgemeiner/direktstaatlicher Operationen nach Regimetyp



(Eigene Darstellung auf Basis des HD-CY.CON)

Nachdem das Bild des überwiegend autokratischen Cyberangreifers gegenüber konventionell überlegenen Demokratien sowie die überwiegend autokratische, offensive Cyberproxy-Nutzung durch den Datensatz bestätigt wurden, gilt es nun, die am häufigsten attribuierten Cyberangreifer zu untersuchen. Dies ist notwendig, um zunächst über absolute Häufigkeiten die beiden aktivsten Autokratien im Cyberspace zu identifizieren und in einem nachgelagerten Schritt deren Proxy-Nutzung auf hinreichende Varianzen für die bereits genannten Kategorien des Zielprofils, Operations-Typs, Offline-Konflikt-Niveaus etc. zu überprüfen. Ist dies der Fall, gilt die autokratische Fallauswahl als abgeschlossen.

Tabelle 9 listet die acht autokratischen Staaten auf, denen im HD-CY.CON am häufigsten Proxy-Operationen zugesprochen wurden. China liegt mit 105 Fällen an der Spitze, gefolgt von Russland mit 59 sowie Iran mit 52 und Nordkorea mit 33 Fällen. Weiter abgeschlagen mit zwölf sowie zehn Vorfällen rangieren Syrien und Vietnam auf dem fünften und sechsten Platz. Dieses Resultat erscheint gemäß der bisherigen Forschungsliteratur zu Cyberkonflikten wenig überraschend. So werden die vier erstgenannten Länder regelmäßig als die ›üblichen Verdächtigen‹ im Falle von Cyberoperationen genannt, jedoch mit regelmäßig unterschiedlichen Angriffsprofilen (Farwell und Rohozinski 2011; Maness und Valeriano 2016b; Rugge 2018).

Tabelle 9: Autokratien nach Häufigkeit der Proxy-Attribution als Angreifer

Rang	Land	Fallanzahl
1	China	105
2	Russland	59
3	Iran	52
4	Nordkorea	33
5	Syrien	12
6	Vietnam	10
7	Vereinigte Arabische Emirate	5
8	Türkei	3

(Eigene Darstellung auf Basis des HD-CY.CON)

Ein nahezu identisches Bild zeigt sich auch bei der Betrachtung der am häufigsten als allgemein/direktstaatlich verantwortlich gemachten Autokratien (Tabelle 10). Auch hier stehen China und Russland an der Spitze, diesmal vor Nordkorea und dem Iran. Der quantitative Unterschied zwischen China und Russland ist dabei weitaus geringer als im Falle der Proxy-Attributionen. Auffallend ist zudem die für den Iran vergleichsweise hohe Anzahl an Proxy-Operationen im Gegensatz zur eher geringeren Anzahl an allgemein/direktstaatlich attribuierten Cyberoperationen mit iranischer Urheberschaft. Somit könnte für den Iran in erster Linie das Motiv des Ausnutzens der größeren technischen Fähigkeiten nichtstaatlicher AkteurInnen im Gegensatz zu den eigenen staat-

lichen Einheiten für dessen intensive Proxy-Nutzung verantwortlich sein. Für Nordkorea wird die Existenz tatsächlicher Cyberproxys immer wieder angezweifelt: Aufgrund der Zentralisierung des weitgehend vom World Wide Web abgeschotteten Intranets des Landes sowie des exklusiven Zugangs für Mitglieder des Regimes erscheint die Möglichkeit digital ermächtigter, nichtstaatlicher AkteurInnen auf nordkoreanischem Boden eher unwahrscheinlich. Nichtsdestotrotz wurde dem Kim-Regime immer wieder die Nutzung im Ausland stationierter Frontorganisationen wie nordkoreanischen Unternehmen oder Studierenden als Cyberproxys attestiert, was diesem Begriff eher entspricht (Zettl 2022).

Tabelle 10: Autokratien nach Häufigkeit der allgemeinen/direktstaatlichen Attribution als Angreifer

Rang	Land	Fallanzahl
1	China	45
2	Russland	37
3	Nordkorea	15
4	Iran	8
5	Saudi-Arabien	4
6	Vietnam	1
7	Türkei	1

(Eigene Darstellung auf Basis des HD-CY.CON)

Somit werden China und Russland aufgrund ihrer zahlenmäßigen Dominanz in beiden AngreiferInnenkategorien als autokratische Fälle für die empirische Analyse ausgewählt. Da der Anspruch der Arbeit jedoch auch darin besteht, potenzielle Varianzen in der autokratischen Proxy-Nutzung aufzeigen zu können, werden beide Länder nun auf hinreichende Anhaltspunkte hierfür untersucht.

5.2.2 Autokratische Fallauswahl: China und Russland im Vergleich

Im relativen Vergleich unterscheiden sich die chinesischen und russischen Cyberoperationsformen nicht signifikant voneinander (Abbildung 17). So wurde für beide Länder der Incident-Typ des Data Thefts mit und ohne Hijacking am häufigsten kodiert. Im Falle der Disruption-Kategorie, sowohl ohne (zumeist DDoS-Operationen) als auch mit Hijacking (z.B. Wiper-Operationen), rangiert Russland jedoch vor China, trotz insgesamt geringerer Fallzahlen mit staatlicher Involvierung. Gleiches gilt für die Unterkategorie des Data Thefts + Doxing: Dieser Incident-Typ wurde ausschließlich russischen Proxys zugesprochen, mit sieben Vorfällen im Untersuchungszeitraum. Somit wiesen lediglich 2,86 Prozent der chinesischen Proxy-Operationen einen disruptiven Charakter auf, im

Gegensatz zu 25,42 Prozent auf russischer Seite. Da Data Theft mit oder ohne Hijacking einen Großteil der korrespondierenden Cyberspionage-Kategorie ausmacht und diese als prävalente Operationsform für nahezu alle Staaten angesehen werden kann (Georgieva 2020), wird die aufgezeigte Varianz zwischen China und Russland auf der Ebene der disruptiveren Operationsformen als hinreichend für deren Fallauswahl betrachtet.[12]

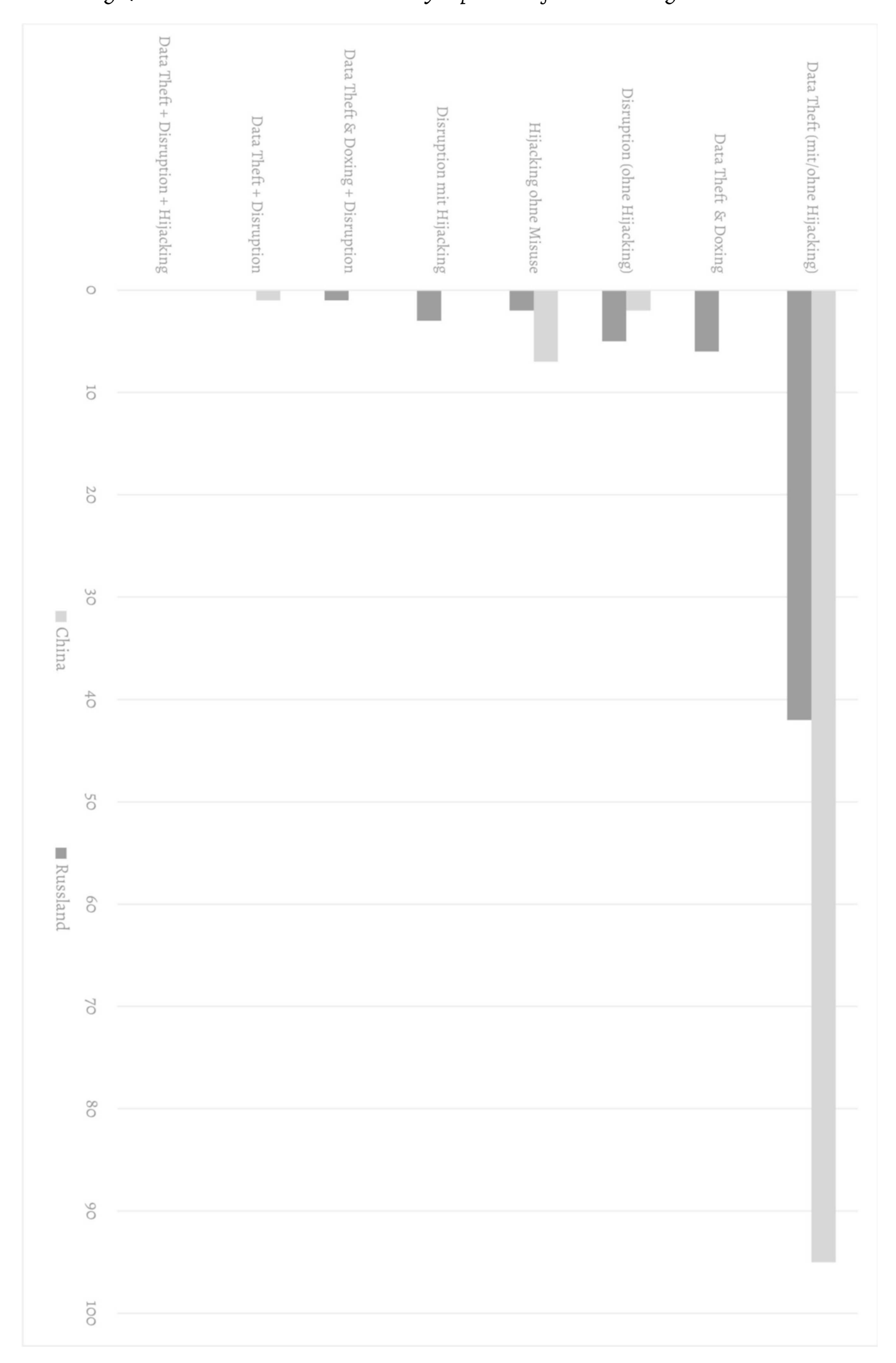
Als zweite Vergleichskategorie dienen die jeweils anvisierten Ziel-AkteurInnen/Bereiche (Abbildung 18): Auch hier ähneln sich die relativen Häufigkeiten chinesischer und russischer Cyberproxy-Operationen über die jeweiligen Zielkategorien weitgehend. So stehen für beide Autokratien politische/staatliche AkteurInnen an erster Stelle. Auch dieser Befund korrespondiert mit der erwähnten Omnipräsenz staatlicher Spionage im Cyberspace. Die Betrachtung der vonseiten chinesischer Proxys am zweithäufigsten anvisierten Unternehmen offenbart jedoch Unterschiede zum russischen Zielprofil. So waren unter den Zielen russischer Proxy-Operationen weitaus seltener Unternehmen zu finden (nur in 16,9 Prozent der Proxy-Vorfälle, im Gegensatz zu 40,0 Prozent für China). Der russische Fokus schien dagegen aus relativer Sicht stärker auf politische/staatliche Ziele ausgerichtet gewesen zu sein (diese waren in 59,3 Prozent der Proxy-Operationen unter den anvisierten Zielen, im Vergleich zu 47,6 Prozent für China). Kritische Infrastrukturen visierten beide Länder relativ ähnlich stark an (27,6 Prozent für China; 22,0 Prozent für Russland), ebenso wie die Zivilgesellschaft (China: 12,4 Prozent; Russland: 16,9 Prozent) und Medien/JournalistInnen (China: 7,6 Prozent; Russland: 16,9 Prozent). Die beiden letztgenannten Zielgruppen prägten das russische Zielportfolio somit im Vergleich etwas stärker als das Chinesische. In den Fallstudien wird auf zeitliche Varianzen in dieser Zielauswahl genauer eingegangen.

Bei der Betrachtung der anvisierten Ziele lohnt es sich, die beiden Metakategorien der politischen/staatlichen Ziele sowie der kritischen Infrastrukturen differenzierter zu betrachten. Abbildung 19 zeigt auf, dass nationale Regierungen, deren Behörden und Ministerien im Falle beider Länder am häufigsten zum Opfer von Cyberproxy-Operationen wurden. Dieser Befund gilt jedoch auch für den Iran und Nordkorea und verdeutlicht die exponierte Stellung von Regierungen sowie nationalen Ministerien im politischen Entscheidungsprozess aller Länder sowie als anvisierte Spionageziele. Auf dem zweiten Platz der politischen/staatlichen Subkategorien folgen militärische AkteurInnen/Institutionen, die absolut gesehen von beiden Autokratien in identischem Umfang anvisiert wurden. Aus relativer Perspektive nimmt diese Zielkategorie für russische Proxy-Operationen (15,3 Prozent) eine etwas bedeutendere Stellung ein als für China (8,6 Prozent). Gleiches gilt für ausländische Botschaften (Russland: 10,2 Prozent, China: 2,9 Prozent) sowie Wahlinfrastruktur/politische Ziele im Rahmen nationaler Wahlen (Russland: 5,1 Prozent; China: 1,9 Prozent).

---

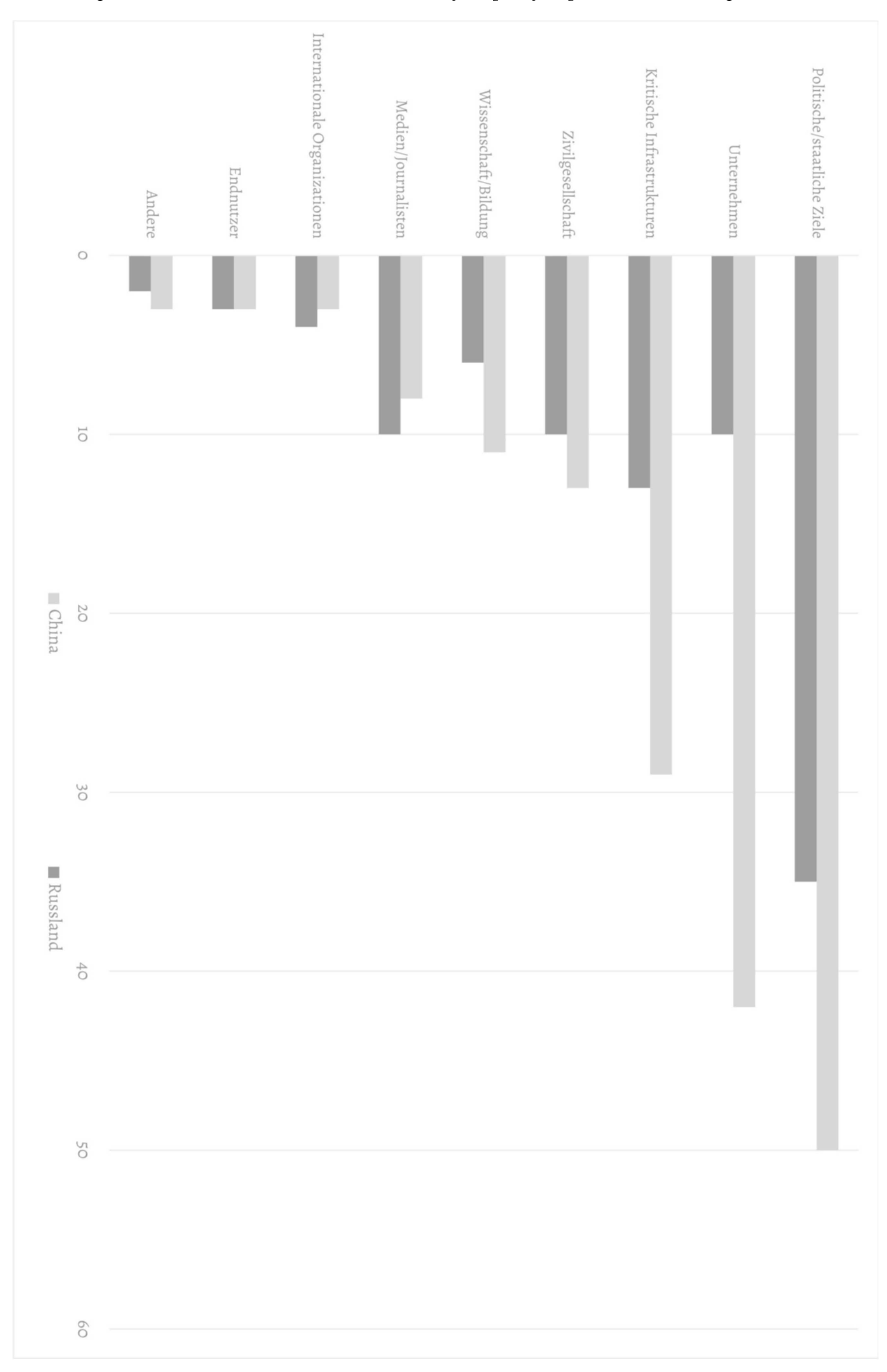
12 Die sieben Fälle von chinesischem Hijacking ohne berichteten Misuse könnten auch in den Bereich der (vorbereitenden) Cyberspionage fallen, andererseits jedoch auch als ›Beachheads‹ im Zielsystem für zukünftige Sabotage-Akte fungieren.

Abbildung 17: Chinesische und russische Proxy-Operationsformen im Vergleich



(Eigene Darstellung auf Basis des HD-CY.CON)

Abbildung 18: Ziele chinesischer und russischer Cyberproxy-Operationen im Vergleich



(Eigene Darstellung auf Basis des HD-CY.CON)

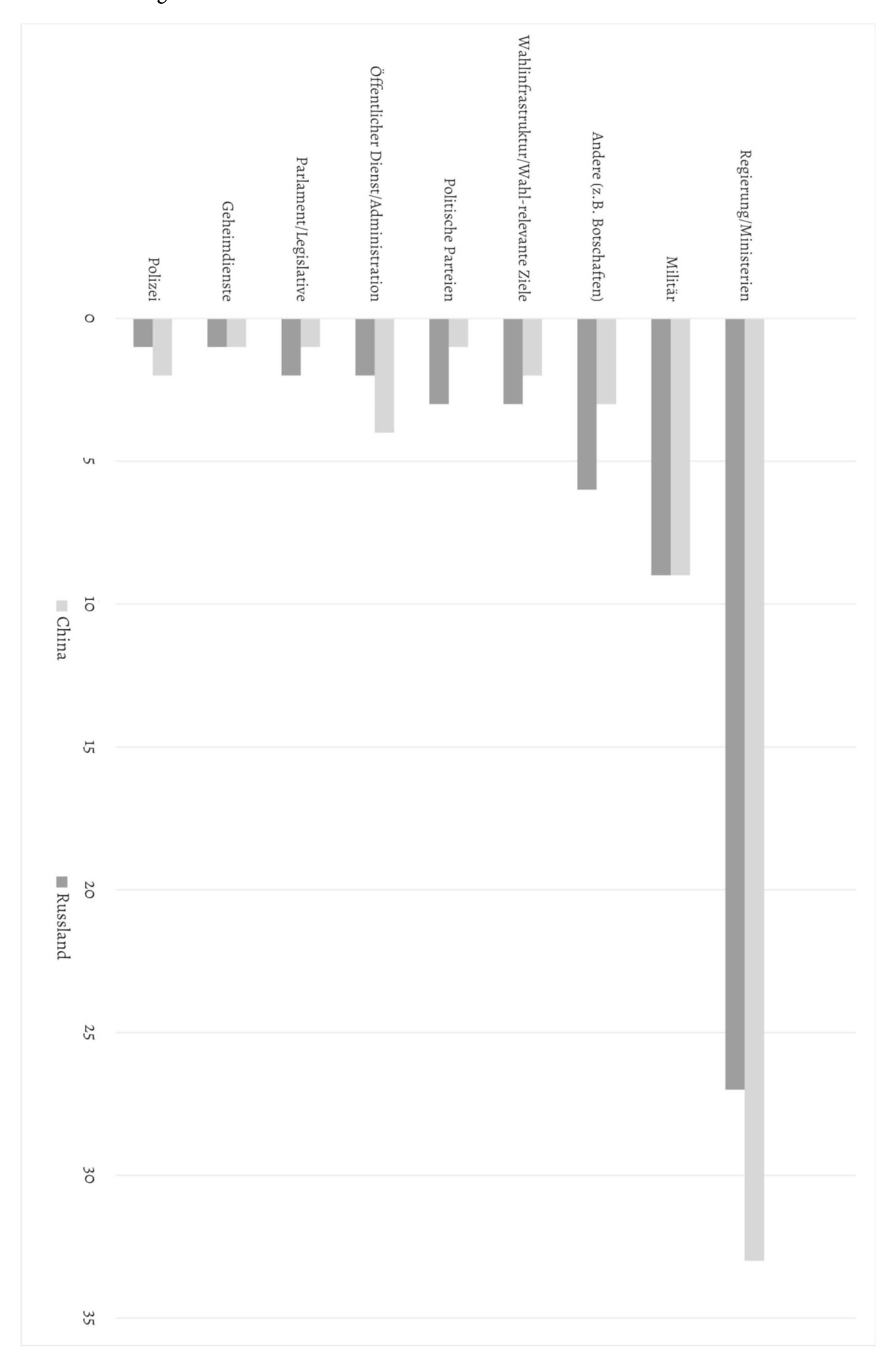
Aufseiten der kritischen Infrastrukturen zeigt sich vor allem für die russischen Cyberproxy-Operationen ein weitgehend ausgeglichenes Bild (Abbildung 20). Keine der gelisteten Untereinheiten setzt sich quantitativ deutlich von den anderen ab. Im Gegensatz dazu lässt sich für die chinesischen Proxy-Operationen ein Muster in Richtung des Verteidigungssektors erkennen, der sich deutlicher von den übrigen Kategorien abhebt. Die anvisierten Rüstungsunternehmen müssen dabei stärker im Lichte der propagierten Einheit zwischen wirtschaftlicher und politischer Spionage betrachtet werden. So argumentierte das kommunistische Regime in der Vergangenheit immer wieder damit, dass sich seine Zielsetzungen im wirtschaftlichen Bereich von der Stärkung der nationalen Sicherheit nicht so ohne Weiteres trennen ließen, wie von demokratischen Ländern wie den USA behauptet. Demnach könne Data Theft auch gegen wirtschaftlich anmutende Ziele zum Zwecke der als eher legitim erachteten politischen Cyberspionage zum Einsatz kommen (Lotrionte 2014, S. 460–462).

Weitere bedeutsame Unterschiede könnten zudem die durch China anvisierten Ziele des Gesundheitssektors sowie auf russischer Seite des Chemiesektors darstellen. Bei ersteren ist – für einen ausgeweiteten Untersuchungszeitraum aufgrund der Covid-19-Pandemie und nicht zuletzt aufgrund der weitverbreiteten Anwendung des chinesischen Impfstoffs vor allem in Dritte-Welt-Ländern – von einem noch stärkeren Zuwachs auszugehen. So wurden seitens der USA im Juli 2020 Anklagen gegen mutmaßlich chinesische Akteure veröffentlicht, denen Spionage-Akte gegen Impfstoff entwickelnde Biotechnologie-Unternehmen angelastet wurden (Bing und Taylor 2020).

Auf russischer Seite könnten die beiden Fälle gegen Unternehmen oder Laboratorien im chemietechnologischen Bereich ebenfalls ein Muster andeuten, das mit dem Einsatz chemischer Kampfstoffe gegen RegimegegnerInnen in Verbindung stehen könnte. Des Weiteren wird für die beiden autokratischen Fallstudien bei der Interpretation der anvisierten Ziele relevant sein, welche Form von Cyberoperationen jeweils angewandt wurde. So erschließt sich im Falle von Telekommunikationsdienstleistern oder des Verteidigungssektors als Ziele stärker ein Fokus auf Cyberspionage, während für Bestandteile nationaler Elektrizitätsnetzwerke oder Transportunternehmen eine Sabotage-Motivation disruptiverer Cyberoperationen plausibler erscheint.

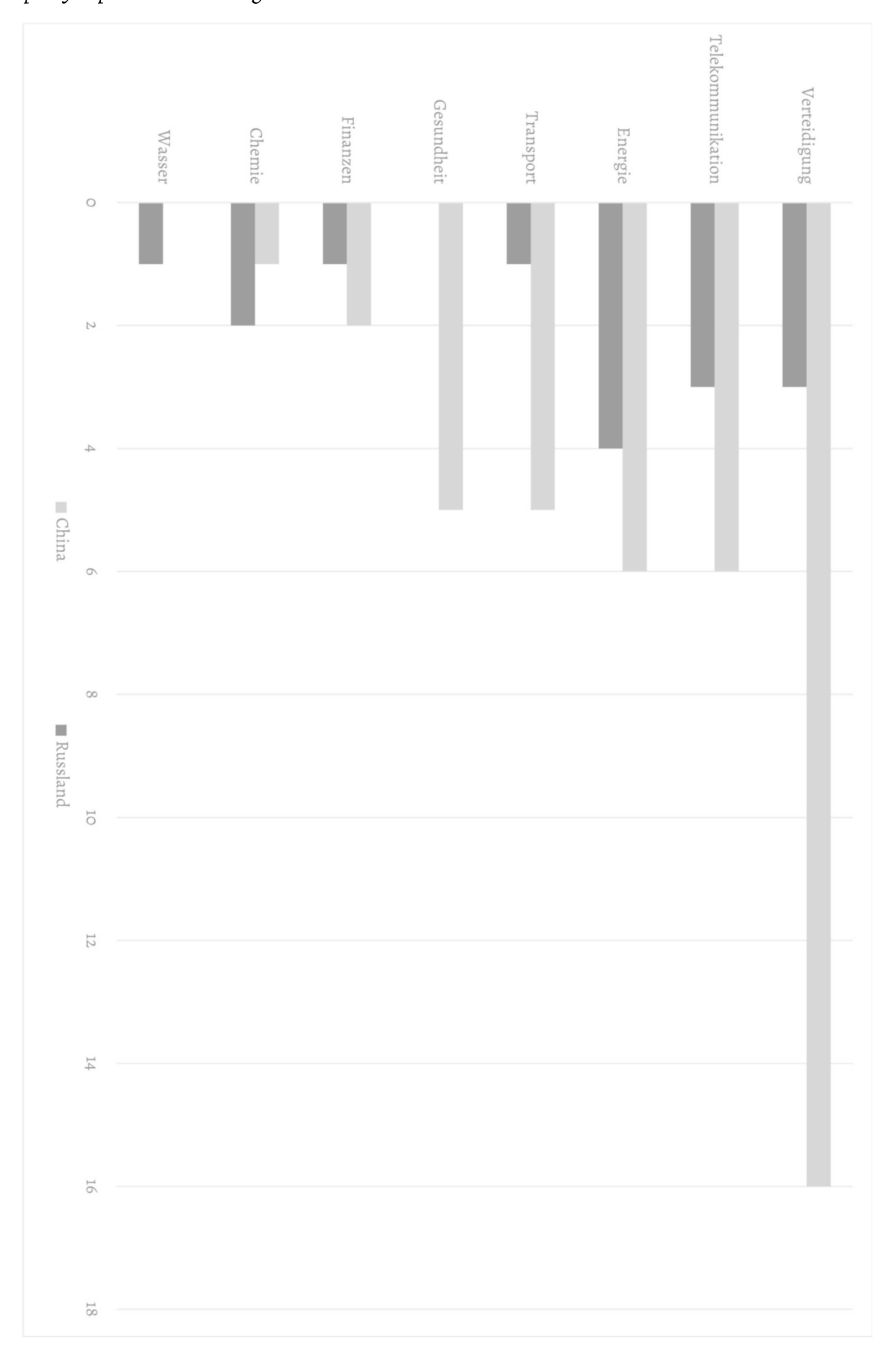
Als weitere Vergleichskategorie dienen die erfassten Cyberproxyoperationen mit affiliierten konventionellen Konflikten (Abbildung 21). Für beide Autokratien zeigt sich, dass die Anzahl an zugeordneten konventionellen Konflikten für China relativ gesehen höher ist als für russische Proxy-Operationen (39,0 Prozent; Russland: 20,3 Prozent). Somit könnte vermutet werden, dass China seine Cyberproxys deutlich häufiger zur Komplementierung von Konfliktdynamiken auf der analogen Ebene einsetzt und Russland dagegen den Cyberspace stärker als isolierten Konfliktaustragungsraum nutzt. Bei zusätzlicher Betrachtung des Anteils der gewaltsamen Konflikte der 41 chinesischen und 12 russischen Cyberoperationen mit kodiertem konventionellem Konflikt erscheint diese Argumentation weniger plausibel: Dieser beträgt für chinesische Proxy-Operationen lediglich 26,8 Prozent von den Fällen mit kodierten konventionellen Konflikten, für russische StellvertreterInnen-Einsätze im Cyberspace mit kodiertem konventionellen Konflikt dagegen 58,3 Prozent. Vor allem im Hinblick auf die Analyse des varianten Einflusses des allgemeinen Konfliktniveaus als IV verspricht dieser Befund von besonderem Interesse zu sein.

Abbildung 19: Subtypen politischer/staatlicher Ziele chinesischer und russischer Cyberproxyoperationen im Vergleich



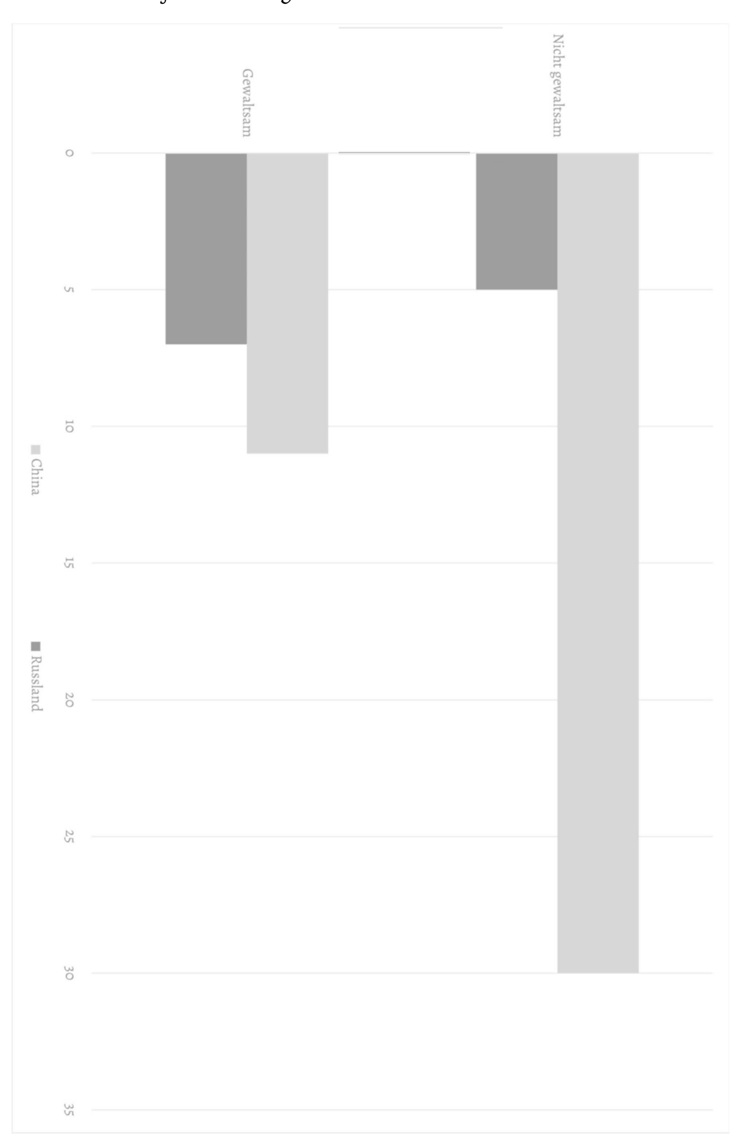
(Eigene Darstellung auf Basis des HD-CY.CON)

Abbildung 20: Subtypen kritischer Infrastrukturen als Ziele chinesischer und russischer Cyberproxy-Operationen im Vergleich



(Eigene Darstellung auf Basis des HD-CY.CON)

Abbildung 21: Chinesische und russische Cyberoperationen mit affiliierten konventionellen Konflikten im Vergleich



(Eigene Darstellung auf Basis des HD-CY.CON);
**Lesehilfe: Für 30 chinesische Proxyoperationen wurde ein entsprechender Konflikt des HIIK-Konfliktbarometers kodiert. Hiervon waren elf gewaltsam (HIIK-Intensitätsstufen 3–5).*

Zusammenfassend stellen China und Russland die beiden Autokratien im Datensatz dar, denen am häufigsten sowohl Proxy- als auch allgemeine/direktstaatliche Cyberoperationen zugesprochen wurden. Die komprimierte Übersicht der Zahlen im Hinblick auf weitere Vergleichskategorien deutete dabei bedeutende Varianzen hinsichtlich der AV I, hiermit im Zusammenhang stehend jedoch auch der AV II, an. Besonders bezüglich des zu analysierenden Einflusses der IV stellen die beiden Autokratien geeignete Fälle dar. Neben diesen inhaltlichen Varianzen spricht aus forschungspragmatischer Sicht die relativ große zeitliche Abdeckung des Untersuchungszeitraums für diese beiden Länder als Vergleichsfälle (China ab 2003; Russland ab 2007). Diese im Vergleich zum Iran oder Nordkorea zeitlich sowie quantitativ erhöhte Informationsgrundlage wird auf qualitativer Ebene durch einen bereits noch umfassender bearbeiteten Forschungsstand zum chinesischen und russischen Verhalten im Cyberspace komplettiert. Da in der vorliegenden Arbeit ein eigenständiges, neues Erklärungsmodell entwickelt wird, erscheint das Testen der grundlegenden Annahmen auf einer möglichst breiten Datenlage als gebotenes Vorgehen. Nichtsdestotrotz sollten bei einer weitgehenden Bestätigung des Ansatzes die Kausaldynamiken auf weitere Fälle angewandt werden, um deren Generalisierbarkeit besser bewerten zu können.

5.2.3 Kennzahlen politischer und technischer Attributionen im HD-CY.CON

Nachdem China und Russland als autokratische Fallbeispiele ausgewählt wurden, erfolgt das gleiche Vorgehen nun auf demokratischer Seite.

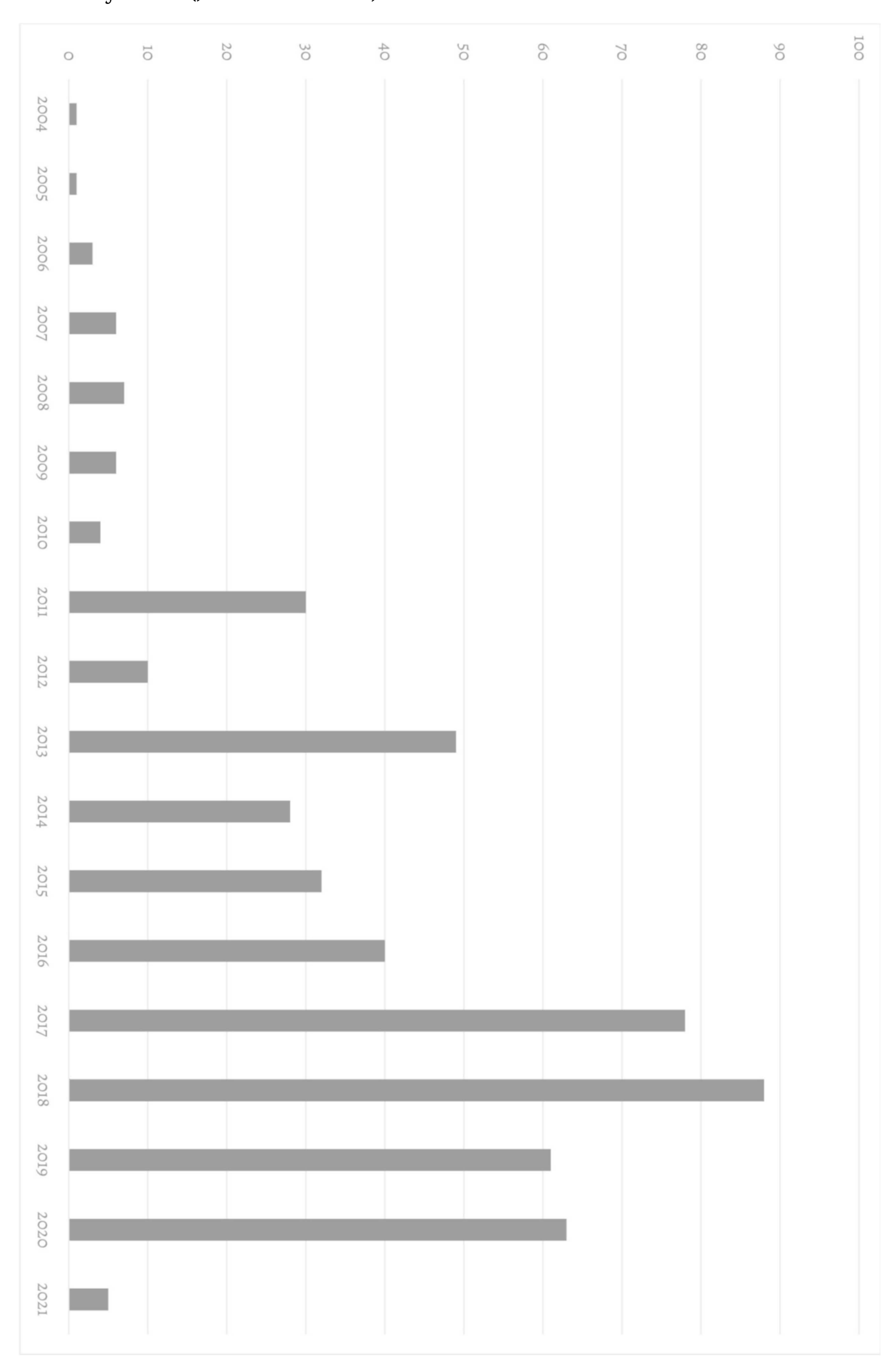
Zunächst wird nochmals auf die beiden Abbildungen 12 und 13 rekurriert. Diese demonstrierten zum einen, dass eine offensive Cyberproxy-Nutzung in der Tat eine autokratische Präferenz ist, andererseits widerlegten sie die Vorstellung eines demokratischen ›Cyberfriedens‹ zumindest monadischer Art. Demokratien sind sehr wohl im Cyberspace aktiv, jedoch in erster Linie durch Cyberspionage und im Falle disruptiverer Operationsformen nach öffentlichem Erkenntnisstand ausschließlich gegenüber Autokratien. Die Enthüllungen Edward Snowdens verdeutlichten die prinzipielle Bereitschaft demokratischer Staaten wie der USA und Großbritannien, sukzessive an der Kapazitätserweiterung solcher ›D-Weapons‹ zu arbeiten (Appelbaum et al. 2015). Plausible Deniability bzw. Verschleierung dient hierbei jedoch in erster Linie nicht der Geheimhaltung der eigenen Verantwortlichkeit, sondern bei Cyberspionage bereits der Detektion der Operation an sich. Naturgemäß wird durch eine erschwerte Detektion einer Cyberoperation auch die Verantwortlichkeit eines Akteurs verschleiert. Nichtsdestotrotz legen die vergleichsweise hohen Zahlen an allgemein/direktstaatlich attribuierten Cyberoperationen mit mutmaßlich demokratischer Herkunft nahe, dass es diesen weniger um die Aufrechterhaltung einer scheinbaren Nichtbeteiligung im Vergleich zu autokratischen Staaten ging. Dies betrifft vor allem disruptive Operationen gegen mutmaßliche ›Schurkenstaaten‹: Die Verletzung deren Souveränität durch einen Cyberangriff wird seitens des ausübenden demokratischen Staates als legitimer erachtet. Grundlage dafür sind die im Rahmen der internationalen, bislang liberal geprägten Weltordnung geteilten Norm- und Wertvorstellungen demokratischer Staaten. Im Gegensatz dazu sind sich Autokratien zumeist bewusst, dass ihre disruptiven Cyberoperationen diesen widersprechen, insbesondere, weil sie zumeist gegen dominante Demokratien

gerichtet sind. In einem kontrafaktischen Gedankenspiel könnte argumentiert werden, dass die USA nach den Snowden-Enthüllungen vermehrt auf tatsächliche Cyberproxys hätten zurückgreifen können, um sich in Zukunft vor ähnlichen Reputationsverlusten besser schützen zu können. Die Daten des HD-CY.CON zeigen jedoch, dass die USA vielmehr im Laufe der Jahre proaktiver bezüglich der eigenen Cyberoperationen und deren Veröffentlichung geworden sind, was somit gegen die Übertragung der autokratischen Proxy-Nutzungslogik auf Demokratien spricht.

Demokratien teilen also die Präferenz autokratischer Staaten für offensive Cyberproxys nicht. Somit gilt es nun deren konzeptualisierte, defensive Cyberproxy-Nutzung anhand des Gesamtdatensatzes zu überprüfen. Abbildung 22 zeigt die Attribution von staatlichen und staatlich gesponserten AngreiferInnen im Verlauf der Zeit. Das jeweilige Jahr bezieht sich in diesem Falle auf den Zeitpunkt der getätigten Attribution und damit nicht zwingend auch auf das Jahr des Operationsbeginns. Auch hier werden zwei Entwicklungen des Cyberkonfliktaustrags sowie der Berichterstattung/öffentlichen Kommunikation deutlich: Die Anzahl an attribuierten Cyberoperationen mit staatlicher Involvierung stieg seit 2004 stetig und mit wenigen, zeitweiligen Rückgängen an. Der Höhepunkt wurde vorläufig 2018 erreicht. Dies spricht zum einen für ein allgemein gesteigertes Attributionsengagement, andererseits für ein grundlegend erhöhtes Cyberkonfliktniveau auf staatlicher Ebene. Hinzu kommen die auf staatlicher Seite steigenden Attributionskapazitäten vor allem geheimdienstlicher AkteurInnen, die ebenfalls zu diesem signifikanten Anstieg beigetragen haben dürften (Mueller et al. 2019).

Für das Erkenntnisinteresse der Arbeit ist zudem von Bedeutung, inwiefern sich der zeitliche Abstand zwischen dem identifizierten Startjahr der Cyberoperation und dem Jahr der öffentlichen Attribution im Verlauf der Zeit verändert hat. Abbildung 23 zeigt diesbezüglich kein eindeutiges zeitliches Muster auf. Insgesamt stieg die zeitliche Differenz zwischen Attributionsjahr und Operationsstartjahr im Zeitverlauf jedoch an. Die Zahlen für die Jahre 2020 und 2021 zeigen den stärksten Anstieg, sind gleichzeitig jedoch am unvollständigsten, da sie sich nur auf Attributions- und nicht auf Operationsstartjahre beziehen. Insofern wäre hier für eine Erweiterung des Datensatzes um die Startjahre 2020 und 2021 von einem Absinken der zeitlichen Differenz auszugehen.

Abbildung 22: Die Attribution von staatlichen und staatlich gesponserten AngreiferInnen im Verlauf der Zeit (Jahr der Attribution)



(Eigene Darstellung auf Basis des HD-CY.CON)

Nichtsdestotrotz sind im Schaubild folgende Aspekte von Interesse:

1. Da sich der staatlich geprägte Cyberkonfliktaustrag erst ab Mitte der 2000er Jahre etablierte, erscheint es nachvollziehbar, dass sich die Attributionen der nachfolgenden Jahre aufgrund des regelmäßigen Fehlens solcher Ereignisse im Zeitraum zuvor auf kürzlich erfolgte Cyberoperationen beziehen (müssen).
2. Dennoch scheinen die absoluten Fallzahlen für Cyberoperationen auch mehrere Jahre nach dem untersuchten Startjahr noch nicht zwingend final erfassbar zu sein. Im Gegensatz zur konventionellen Konfliktforschung repräsentieren diese daher stärker ein vorläufiges Ergebnis.
3. Trotz gestiegener Detektions- und Attributionskapazitäten vor allem staatlicher AkteurInnen schaffen es einzelne CyberangreiferInnen immer wieder, für einen relativ langen Zeitraum unerkannt zu bleiben. Dies setzt allerdings die Annahme voraus, dass zwischen der Detektion und öffentlichen Attribution der jeweiligen Operation ein möglichst kurzer Abstand lag. Dementsprechend wäre eine zweite Erklärung hierfür, dass AkteurInnen regelmäßig aufgrund zuvor fehlender Evidenz oder veränderter eskalationsstrategischer Kalküle bereits seit längerem detektierte Cyberoperationen erst nach einigen Jahren öffentlich attribuieren.

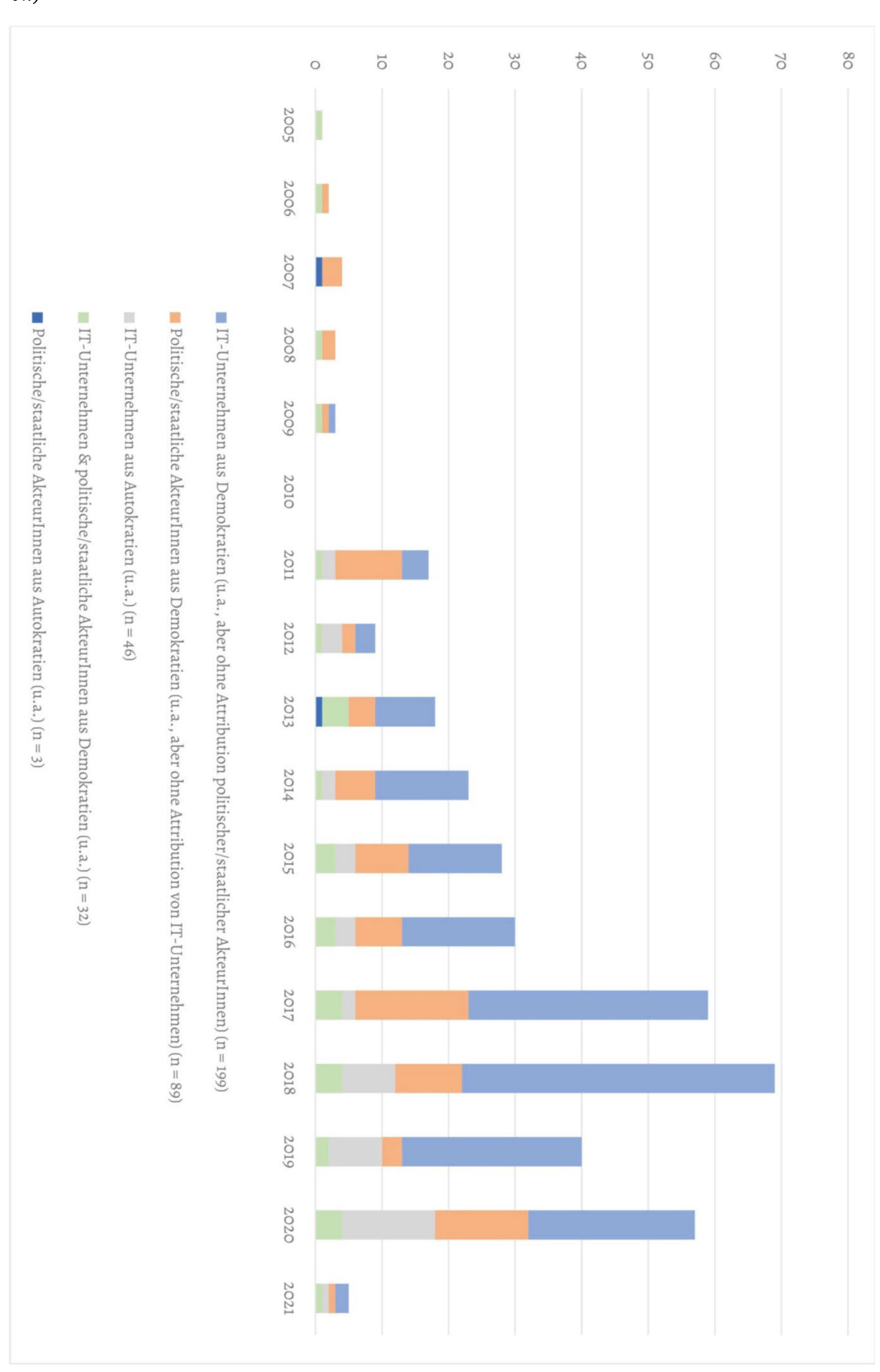
Sind aber auch tatsächlich regelmäßig private IT-Unternehmen für derartige Attributionen verantwortlich? Oder lässt sich die These von der defensiven Nutzung demokratischer Cyberproxys auf Grundlage des HD-CY.CON bereits auf der Ebene des Gesamtdatensatzes so nicht halten? Wie Abbildung 24 aufzeigt, stehen IT-Unternehmen tatsächlich an erster Stelle der im Datensatz erfassten Attributionsquellen für Operationen mit staatlicher Beteiligung (199 Attributionen). Auf dem zweiten Rang folgen politische/staatliche AkteurInnen aus Demokratien mit 89 Fällen. Die erfassten 46 Fälle autokratischer IT-Firmen könnten nun die These aufwerfen, dass die defensive Cyberproxy-Nutzung doch weniger ein demokratisches als ein regimetypenübergreifendes Phänomen darstellt. Wird jedoch in Betracht gezogen, dass für diese Zahl in erster Linie die russische, international etablierte IT-Firma Kaspersky verantwortlich ist, relativiert sich die Plausibilität der Übertragung des defensiven Cyberproxy-Konzepts auf autokratische Staaten deutlich.[13] Auffällig ist zudem die geringe Zahl an erfassten Attributionen politischer/staatlicher AkteurInnen aus Autokratien.

13 Für China gibt es stattdessen sogar Evidenzen, dass technische Berichte der nationalen IT-Unternehmen besonders dann seitens der Regierung zensiert werden, wenn die USA oder die NATO als Urheber der aufgedeckten Cyberoperationen vermutet werden (Cimpanu 2021a), was gegen eine durch nationale IT-Unternehmen als Proxys intendierte Signaling-Funktion spricht.

Abbildung 23: Durchschnittliche Differenz Attributionsjahr – Startjahr der Operation

(Eigene Darstellung auf Basis des HD-CY.CON)
Lesehilfe: Die im HD-CY.CON im Attributionsjahr 2018 erfassten Cyberoperationen mit attribuierter, staatlicher Involvierung auf der AngreiferInnen-Seite (allgemein/direktstaatlich oder staatlich gesponsert) starteten im Durchschnitt zwei Jahre zuvor.

Abbildung 24: Angriffe mit staatlicher Beteiligung nach Attributionsquellen (Jahr der Attribution)



(Eigene Darstellung auf Basis des HD-CY.CON)

Anmerkung: Die Zahlen beziehen sich auf einzelne und kombinierte Attributionsquellen für Fälle, in denen diese jeweils eine staatliche Involvierung auf der AngreiferInnenseite attribuiert haben, das Initiator-Country kann dabei jedoch unbenannt geblieben sein.

In der nachfolgenden Tabelle werden die Attributionsakte mit mindestens einer positiven Kodierung, entweder des Herkunftslandes oder der AngreiferInnen-Kategorie (auch nichtstaatliche AkteurInnen), entsprechend der Herkunftsländer der hierfür verantwortlichen IT-Unternehmens aufgeschlüsselt. Wenig überraschend rangiert die USA mit ihren zahlreichen IT-Unternehmen, die im Threat-Research-Bereich führend sind, mit 217 Attributionsakten deutlich an erster Stelle. Es folgt Russland mit 49 Attributionen, wofür in erster Linie das Unternehmen Kaspersky verantwortlich war.[14] Auf dem dritten Platz rangiert Israel, das sich mit 31 privatwirtschaftlichen Attributionen zahlenmäßig noch deutlich von den nachfolgenden Ländern absetzt. Aufseiten der Autokratien sticht ansonsten nur noch China mit acht verzeichneten Attributionen heraus. Die Attributionspraxis privater IT-Unternehmen war somit im Untersuchungszeitraum vornehmlich demokratisch geprägt. Eine Vielzahl an demokratischen Ländern kann dabei zumindest eine international aktive und mit entsprechender Reputation versehene IT-Firma aufweisen. Für Japan ist dies etwa TrendMicro, für die Slowakei ESET und für Rumänien Bitdefender.

Tabelle 11: Die Herkunftsländer attribuierender IT-Unternehmen

Rang	Land	Attributionsanzahl*	Regimetyp
1	USA	217	Demokratie
2	Russland	49	Autokratie
3	Israel	31	Demokratie
4	Slowakei	15	Demokratie
5	Japan	10	Demokratie
6	China	8	Autokratie
7	Großbritannien	6	Demokratie
8	Niederlande	5	Demokratie
9	Rumänien	5	Demokratie
10	Finnland	4	Demokratie
11	Spanien	2	Demokratie
12	Taiwan	2	Demokratie
13	Kuwait	2	Autokratie
14	Deutschland	2	Demokratie
15	Indien	1	Demokratie
16	Italien	1	Demokratie
17	Kanada	1	Demokratie

14 Zudem wurde jedoch auch das russische Unternehmen IB-Group als attribuierender Akteur erfasst.

18	Tschechien	1	Demokratie
19	Südkorea	1	Demokratie
20	Iran	1	Autokratie

(Eigene Darstellung auf Basis des HD-CY.CON)
**Inkludiert alle Fälle mit zumindest einer positiven Initiator-Kodierung, also auch solche, in denen entweder nur das AngreiferInnen-Land oder die AngreiferInnen-Art attribuiert wurde. Dabei beziehen sich manche Attributionen auf dieselben Fälle, z.B. im Falle der beiden Attributionen kuwaitischer IT-Unternehmen, in denen ebenfalls ein israelisches IT-Unternehmen als Attribution-Basis verzeichnet wurde.*

5.2.4 Demokratische Fallauswahl: Die USA und Israel als *Best Cases*

Auf der quantitativen Ebene stellen somit die USA und Israel die plausibelsten demokratischen Fallbeispiele für die empirische Analyse dar. Der signifikante Unterschied zwischen den Beobachtungsanzahlen bedarf jedoch einer kritischen Reflexion. Andererseits demonstriert dieser lediglich die extreme Tech-Dominanz von US-Unternehmen, auch im Threat-Research-Bereich. Aufgrund der oftmals beobachteten Signalwirkung des Verhaltens bzw. der Positionierung der USA auf andere demokratische Länder (Ben-Porat 2005, S. 225–226) sollte die Analyse des ›Most-Likely-Case‹ vielmehr zur Erhärtung bzw. Ausdifferenzierung der theoretischen Annahmen genutzt und nicht aufgrund der quantitativen Ausreißerstellung im Sinne defizitärer Vergleichbarkeit verworfen werden.

Israel erscheint aus mehreren Gründen als geeigneter Vergleichsfall:

1. Das Land rangiert hinter den USA und Russland als zweite Demokratie in Tabelle 11;
2. Es weist eine vergleichsweise deutliche Differenz zur nächstplatzierten Demokratie (Slowakei) auf;
3. Israel stellt im Gegensatz zu den meisten der nachfolgenden Demokratien nicht nur ein IT-Unternehmen im HD-CY.CON, sondern gleich sieben;
4. Israel ist auch aufgrund seiner geopolitischen Lage sowie der oftmals berichteten engen Verquickung zwischen dem privaten IT-Sektor sowie staatlichen Sicherheitsorganen eine Art zweiter ›Most-Likely-Case‹ für die neuartige Konzeptualisierung von IT-Unternehmen als defensive Cyberproxys (Swed und Butler 2015; Baram 2017).
5. So wird zudem für die Analyse von Interesse sein, inwiefern sich ein Nexus zwischen der geopolitischen Konfliktsituation in der Region und dem Attributionsverhalten israelischer Unternehmen plausibilisieren lässt, was den für demokratische Cyberproxys schwieriger nachweisbaren Staat-Proxy-Delegationsmodus erhärten würde.
6. Ob die USA und Israel jedoch bislang Ausnahmen in der konzeptualisierten defensiven Cyberproxy-Nutzung darstellen oder ob sich dieser Modus in der Zukunft auch unter weiteren Demokratien verbreitet, könnte Gegenstand weiterer Studien sein.

5.3 Autokratisches Fallbeispiel I: China

»In today's information age, the People's Republic of China has replaced and even improved upon KGB methods of industrial espionage to the point that the People's Republic of China now presents one of the most capable threats to U.S. technology leadership and by extension its national security.«
Dan Verton, zitiert in Hjortdal (2011, S. 2)[15]

In der öffentlichen Wahrnehmung wechselten sich bislang China und Russland als größte Bedrohungen im Cyberspace für Demokratien in den letzten zwanzig Jahren immer wieder ab. China erfuhr insbesondere seit 2010, als deren Spionageoperation Aurora öffentlich wurde, besonders seitens der USA eine gestiegene Aufmerksamkeit (s. das Zitat von Verton). Verstärkt wurde diese China-Rhetorik mit immer stärkeren Bezügen zu dessen angestrebter Kontestation der US-Hegemonie im Technologiesektor unter Donald Trump, nachdem 2016 noch die russische Wahlbeeinflussung als größte Gefahr für die USA und Demokratien im Allgemeinen dargestellt wurde (Dorfman 2020b).

Die nachfolgende Fallstudie hat somit zum Ziel, die Rolle offensiver Cyberproxys in der primär ökonomisch geprägten Instrumentalisierung des Cyberspace durch China zu analysieren. Dabei gilt es zudem, die von westlichen Demokratien abweichende Sichtweise der kommunistischen Partei auf die Trennbarkeit der Bereiche des Politischen und des Ökonomischen herauszuarbeiten. Besonders werden die chinesischen Vorstellungen im regulationspolitischen Bereich sowie die sich daraus ergebenden Konflikte zu demokratischen und, im Falle der EU, zusätzlich supranationalen Governance-Modellen im Mittelpunkt stehen. Aufgrund des zentralen Führungswechsels an der Spitze der Regierung durch Xi Jinpings Amtsübernahme 2013 wird dessen Einfluss auf die chinesische Präferenzkonstellation und somit Proxy-Nutzung von besonderer Bedeutung sein.[16] Im analogen Bereich wurde China deutlich seltener als möglicher oder faktischer Proxy-Auftraggeber behandelt, im Gegensatz zur Union der Sozialistischen Sowjetrepubliken (UdSSR) im Kalten Krieg.[17] Wie, warum und mithilfe welcher AkteurInnen dies im Cyberspace verändert wurde, gilt es nachfolgend zu untersuchen.

---

15 Dan Verton war zum Zeitpunkt der Einreichung der Arbeit für das IT-Unternehmen Cybereason tätig, zuvor arbeitete er für Geheimdienste und als Journalist (Cybereason 2022).

16 Natürlich können sich domestische Präferenzordnungen auch innerhalb einer Legislaturperiode über Zeit verändern, siehe Deutschlands Außenpolitik gegenüber Chinas »*One Belt, One Road*« (OBOR)-Initiative von 2013 bis 2017 (Harnisch 2018).

17 Zwei Ausnahmen stellen dazu Bar-Siman-Tov 1984 und Yeisley 2011 dar: Ersterer untersuchte, inwiefern der Vietnam-Krieg als Proxy-Krieg Russlands und Chinas gewertet werden sollte und zweiterer diskutierte die Möglichkeiten künftiger Proxy-Konflikte ökonomischer Natur zwischen den USA und China auf afrikanischem Boden.

5.3.1 Chinesische Cyberproxy-Operationen (2000–2019): Wer macht was?

»There are only two types of companies – those that know they've been compromised, and those that don't know. If you have anything that may be valuable to a competitor, you will be targeted, and almost certainly compromised.«
Dmitri Alperovitch über chinesische Cyberspionage, zitiert in (Gross 2011)

Wie bereits in den Tabellen 9 und 10 aufgezeigt, verzeichnet der HD-CY.CON 105 Proxy-Operationen mit attribuierter chinesischer Verantwortung und zudem 45 direktstaatlich attribuierte chinesische Cyberoperationen. Keine davon wurde durch China selbst offengelegt, bzw. zu keiner Operation hat sich das Land bekannt.

Für die Analyse der AV I, also der inhaltlichen Funktionen autokratischer Cyberproxys, stellt der HD-CY.CON eine noch zentralere Informationsquelle dar als für die AV II, deren Überprüfung noch umfassender das Hinzuziehen qualitativer Sekundärliteratur erfordert. Somit liegt der Fokus im Folgenden anhand der unter 4.5 vorgestellten Leitfragen zunächst auf den aus dem Datensatz abzuleitenden Funktionen chinesischer Cyberproxys (s. Tabelle 1). Wie das obere Zitat bereits andeutet, kommt chinesischer Cyberspionage gegenüber kommerziellen Zielen eine besondere Bedeutung zu.

5.3.1.1 Chinesische Cyberproxy-Funktionen auf Grundlage des HD-CY.CON

Proxys spielten für chinesische Cyberoperationen bereits seit 2003 eine wichtige Rolle (Abbildung 25): Während jedoch in den ersten fünf verzeichneten Jahren des HD-CY.CON (2000–2004) für China lediglich drei Cyberoperationen mit attribuierter Proxy-Verantwortlichkeit erfasst wurden, stieg deren Anzahl (trotz eines kurzfristigen Rückgangs im Jahr 2012) bis 2017 stetig an und übertraf damit die für China allgemein/direktstaatlich attribuierten Cyberoperationen (außer zwischen 2006 und 2008) in allen Untersuchungsjahren. Die Gesamtzahl chinesischer Cyberoperationen stieg insbesondere ab 2012 stetig an, wofür vor allem der Anteil der Proxyoperationen verantwortlich ist. Ob die für 2018/2019 angedeutete Annäherung zwischen den beiden AngreiferInnenkategorien auch noch in absehbarer Zukunft und nach potenziell hinzugekommenen Operationen für diese Startjahre bestehen bleibt, kann an dieser Stelle nicht beurteilt werden. Besonders auffällig erscheint der Anstieg von 2016 zu 2017, von neun zu 15 erfassten chinesischen Proxyoperationen. Inwiefern für die absolute Zunahme der Operationen insgesamt nach 2012 Xi Jinpings Amtsübernahme als Präsident verantwortlich gemacht werden kann, wird Gegenstand der Analyse der UV sein.

Die fehlende Parallelität der Zu- und Abnahme von Proxy- und direktstaatlichen Operationen könnte darauf hindeuten, dass sie weitgehend getrennt voneinander durchgeführt wurden, mit unterschiedlichen Zielsetzungen und Verantwortlichkeiten im Staatsapparat. Eine weitgehend ähnliche zeitliche Entwicklung hinsichtlich der relativen Zu- oder Abnahme der Cyberoperationen hätte dagegen für eine größere zumindest funktionale Verschränkung der beiden Operationskategorien gesprochen, für die z.B. realpolitische Ereignisse dieselben Aktivitätsmuster auslösen könnten. Eine noch inversere Beziehung der zeitlichen Entwicklungen hätte dagegen eine primär komplementäre Strategie Chinas angedeutet, bei der sich Proxys und direktstaatliche AkteurInnen im Cyberkonfliktaustrag bewusst abwechseln. Dies scheint jedoch zumin-

dest entsprechend der Daten des HD-CY.CON nicht eindeutig der Fall gewesen zu sein, weshalb im Rahmen der Analyse der AV II genauer untersucht werden muss, welche staatlichen AkteurInnen jeweils in der Verantwortung standen und inwiefern deren unterschiedliche Präferenzen und Zielsetzungen dieses Bild erklären können. Von den ca. 37 erfassten chinesischen APT-Gruppierungen mit attribuierter, staatlicher Verbindung wurden von dreien Operationen sowohl als Proxy- als auch als direktstaatliche Operationen attribuiert.[18] Deren allgemein/direktstaatlich attribuierte Operationen werden somit ebenfalls in die nachfolgende Untersuchung aufgenommen.

Für chinesische Cyberproxyoperationen dominierte Data Theft als prävalenter Incident-Type (Abbildung 26).[19] Hijacking diente dabei im Großteil der Fälle als technischer ›Erfüllungsgehilfe‹ für Data Theft. In über 90 Prozent der hier erfassten Fälle kann somit Cyberspionage als das mutmaßliche Ziel chinesischer Proxyoperationen ausgemacht werden, was einen ersten Zuschnitt auf die damit verbundenen Proxyfunktionen bedeutet. Auffällig ist neben den lediglich insgesamt vier Fällen mit (auch) disruptiver Wirkung, dass der Incident-Type des Data Theft + Doxing für China überhaupt nicht verzeichnet wurde. Dies könnte sich aufgrund einer in den letzten Jahren attestierten, aggressiveren und nationalistischeren Diplomatie sowie Außenpolitik Chinas (Stichwort »*wolf-warrior diplomacy*«; Zhu 2020) jedoch für aktuellere Zeiträume ändern.

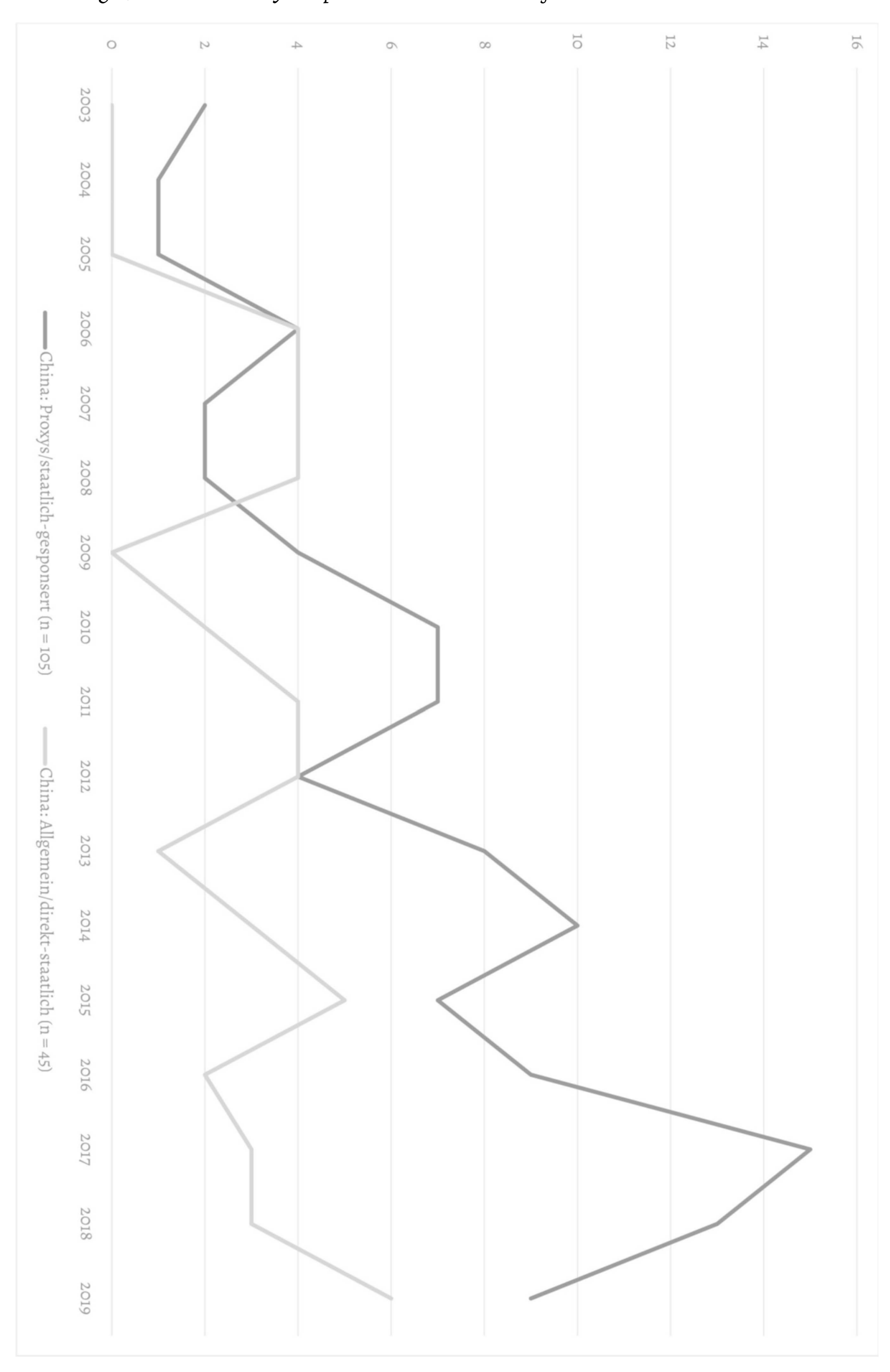
Ein Merkmal chinesischer Cyberspionage-Operationen ist auch deren häufige Langlebigkeit: So dauerten allein 20 der 115 hier erfassten Operationen fünf Jahre oder länger, in einem Fall sogar bis zu 12 Jahre.[20] Verantwortlich hierfür könnte eine erst spät erfolgte Detektion oder Attribution der Operationen gewesen sein. Da bei den besonders lang andauernden Operationen die betroffenen Opfer die AngreiferInnen wohl eher nicht absichtlich haben agieren lassen, kann dies als ein Indikator für die Persistenz chinesischer Proxys gewertet werden, die sich über einen langen Zeitraum in ihren Zielsystemen auszubreiten verstehen.

18 Die genaue Zählung der APT-Gruppierungen gestaltet sich aufgrund der sich teilweise überlappenden, oder auch sich widersprechenden Benennungen seitens verschiedener IT-Unternehmen schwierig, daher wird hier die Einschränkung ›ca.‹ verwendet. Ein Beispiel ist die Attributionsepisode um die Hacks diverser US-Ziele im Jahr 2015 (Anthem, Premera Blue Cross, OPM Hack, United Airlines), für welche mal die der *People's Liberation Army* (PLA) zugeordneten Deep Panda/APT19 und mal der Ministry of State Security (MSS)-Proxy Turbine Panda/APT26 verantwortlich gemacht wurden (Krebs 2015; Gertz 2015; Calian 2020; TeamPassword 2021). Die drei APTs mit sowohl Proxy- als auch allgemein/direktstaatlicher Attribution sind Comment Crew/APT1/Byzantine Candor, Naikon/APT30 und StonePanda/APT10/menupass.

19 Diese sowie alle nachfolgenden Grafiken für China beziehen sich auf alle chinesischen Cyberoperationen mit 2 oder 2,1 als kodierter Initiator-Category (state-sponsored/Proxy-Operationen) plus der zehn als allgemein/direktstaatlich attribuierten Operationen der APTs Comment Crew/APT1/Byzantine Candor, Naikon/APT30 und StonePanda/APT10/menupass (n = 115).

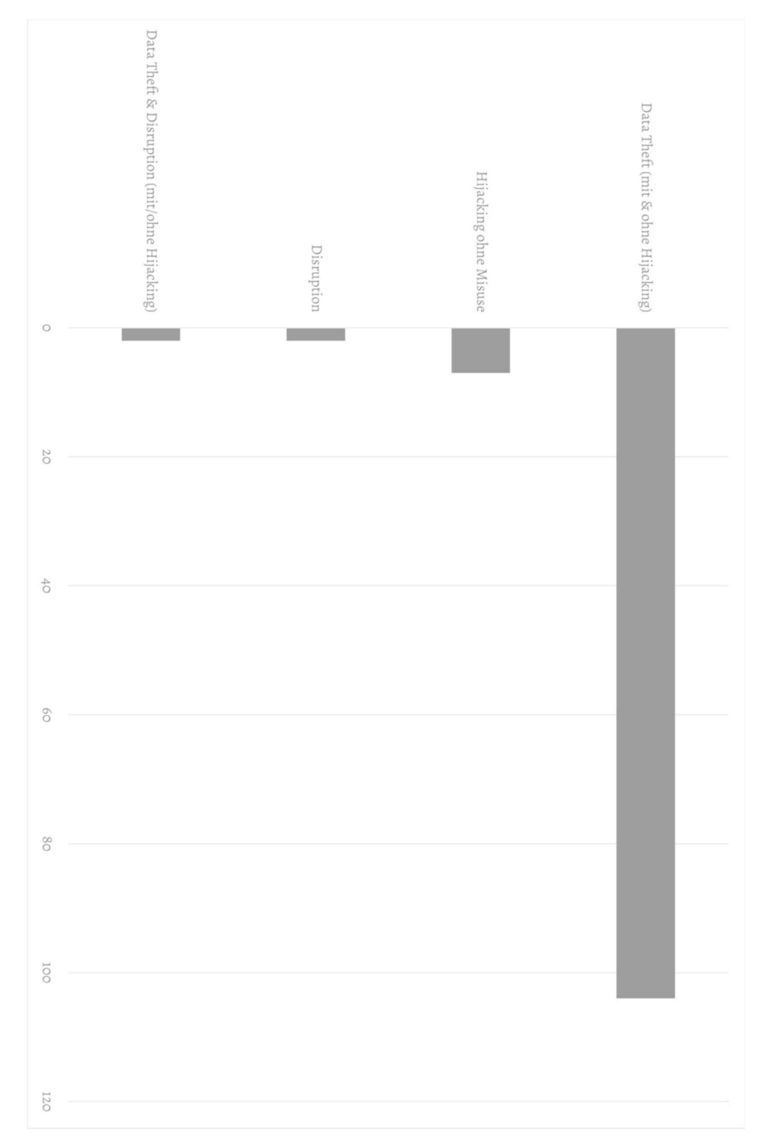
20 Hierbei handelte es sich um eine großangelegte, globale Cyberspionage-Kampagne der Gruppierung Stone Panda/menuPass/APT10 von 2006 bis 2018, gegen die die USA 2018 Anklage erhoben (Barrett 2018). Bei den Zeitangaben ist zudem laut IT-Unternehmen oftmals von Mindestwerten auszugehen, da viele Operationen zum Zeitpunkt der Berichtsveröffentlichung immer noch aktiv waren.

Abbildung 25: Chinesische Cyberoperationen im Zeitverlauf



(Eigene Darstellung auf Basis des HD-CY.CON)

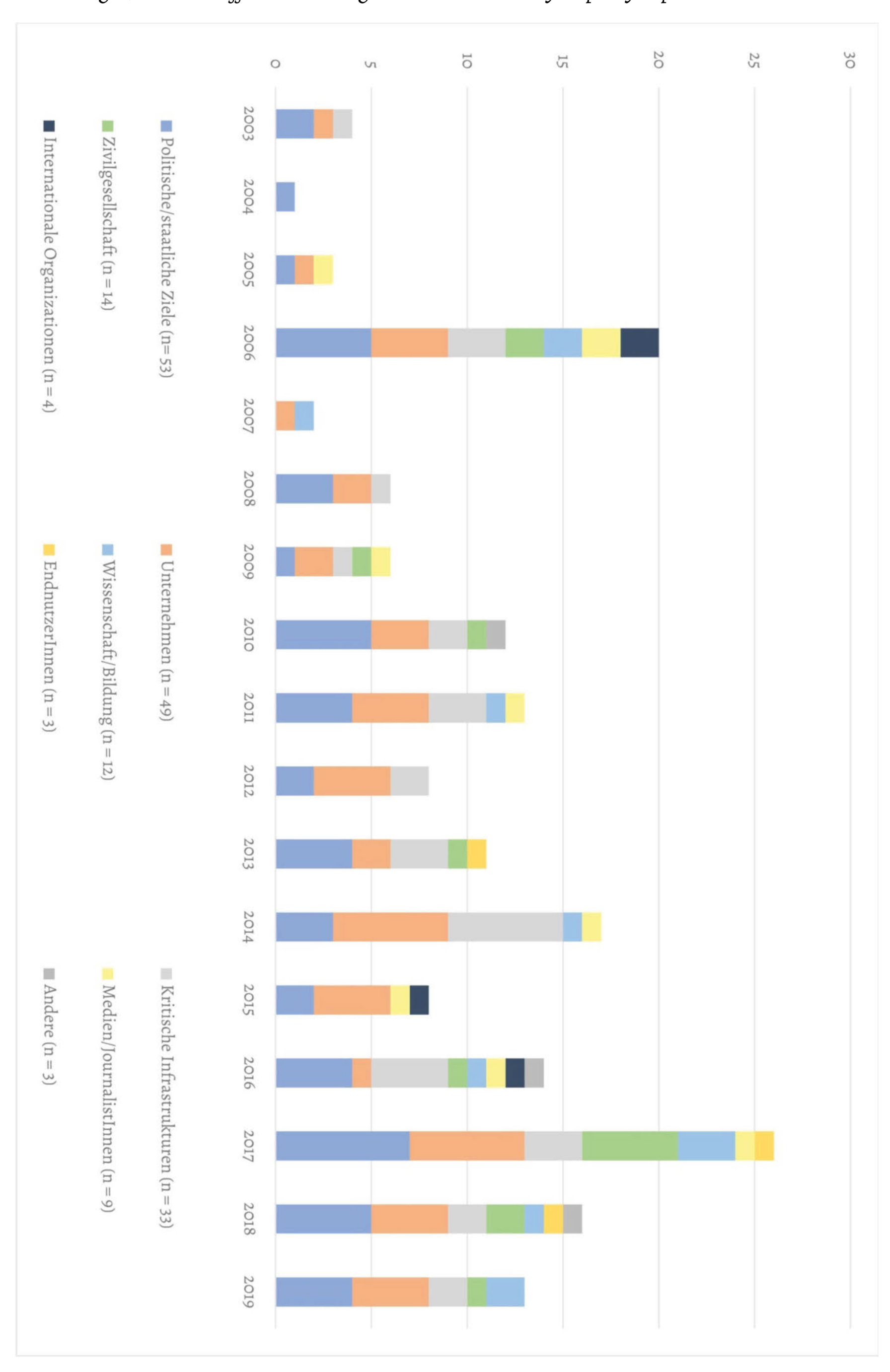
Abbildung 26: Incident-Types chinesischer Cyberproxy-Operationen



(Eigene Darstellung auf Basis des HD-CY.CON)

Um die chinesischen Cyberproxyfunktionen noch spezifischer bestimmen zu können, muss der dominierende Incident-Type des Data Theft in Bezug zu den anvisierten Zielkategorien gesetzt werden (Abbildung 27).

Abbildung 27: Die betroffenen Zielkategorien chinesischer Cyberproxy-Operationen



(Eigene Darstellung auf Basis des HD-CY.CON)

Politische/staatliche Ziele waren mit 53 Operationen am häufigsten unter den anvisierten Opfern, gefolgt von Unternehmen mit 49 und kritischen Infrastrukturen mit 33 Fällen.[21] Mit nun weitaus größerem Abstand folgten die Bereiche der Zivilgesellschaft mit zwölf, Medien/JournalistInnen mit elf sowie Wissenschaft/Bildung mit neun verzeichneten Fällen. Diese Verteilung spricht für eine große Erklärungskraft der allgemeinen, politischen, aber insbesondere der ökonomisch motivierten Cyberspionage als intendierter Proxyfunktion. Der bekannteste Fall politischer Cyberspionage chinesischer Hacker ist der OPM-Hack aus dem Jahr 2015.[22] Dabei gelang es mutmaßlich chinesischen Proxys, Daten von mehreren Millionen aktuellen sowie ehemaligen US-Staatsangestellten, deren Verwandten, BewerberInnen und somit auch US-AgentInnen im Ausland zu erbeuten. Das Ausmaß dieses ›Intelligence-Desasters‹ wurde von US-BeobachterInnen als kaum zu ermessen betitelt, ermöglichte es doch chinesischen Behörden, mithilfe der Daten US-AgentInnen prinzipiell zu identifizieren, diese zu verhaften, zu töten oder aber durch Erpressung zu Doppelagenten werden zu lassen (Dorfman 2020a). Gepaart mit Daten aus anderen Hacks, etwa der Hotelkette Marriott 2014, des Gesundheitsversicherers Anthem (ebenfalls 2014) sowie verschiedener US-Airlines, konnte China somit potenziell ein umfassendes Bild der US-Geheimdienstaktivitäten im In- und Ausland erstellen und darauf basierend verschiedene Schwachpunkte identifizieren und ausnutzen (Dorfman 2020a).

Als zweithäufigste Zielkategorie deuten Unternehmen auf die zentrale Funktion der Wirtschaftsspionage für chinesische Cyberproxys hin. Dieses kann und wird auch seitens der bestehenden Forschung als eine Art zentrales Charakteristikum der chinesischen Entwicklungsstrategie im ökonomischen Bereich im Sinne des bereits erwähnten ›Leapfroggings‹ angesehen (Hjortdal 2011; Iasiello 2016; Gilli und Gilli 2019). In fast der Hälfte der Fälle waren Unternehmen das alleinige Ziel chinesischer Cyberoperationen und können daher noch stärker unter die Rubrik der ›Targeted Operations‹ gefasst werden (Schmitt 2015).[23] Bemerkenswert ist, dass die chinesische Cyberwirtschaftsspionage bereits 2003 im HD-CY.CON erstmals als Startjahr erfasst wird und sich gleichzeitig im Laufe der Jahre quantitativ stetig gesteigert hat. Somit können dieser Proxy-Funktion große Kontinuität und eine längerfristige Perspektive zugesprochen werden.

Das Länderprofil der hierbei anvisierten Unternehmen entspricht deren Führerschaft im Technologie- und Industriebereich, so waren vor allem US-Unternehmen beliebte Ziele chinesischer Cyberspionage. Aber auch weitere Demokratien wie Großbritannien, Deutschland oder Japan wurden im Wirtschaftsbereich kontinuierlich ausspioniert. Auffällig hierbei ist für die USA, dass die öffentlich bekannt gewordenen Spionageoperationen chinesischer AkteurInnen im Jahr 2016 abrupt endeten, 2017 jedoch wieder anstiegen. Auf der Hand liegt, dass hierfür das Obama-Xi-Abkommen

21 Die Akteurskategorien wurden dabei oftmals auch in ein und demselben Fall ausspioniert, weshalb die Aufsummierung der Receiver-Kategorien die Anzahl der Proxy-Operationen weit übersteigt.

22 Den US-Behörden bekannt war der Fall mutmaßlich bereits 2012, dessen genaues Startdatum erscheint dagegen weiterhin unklar (Dorfman 2020a).

23 Auch Teile der kritischen Infrastrukturen, z.B. AkteurInnen aus dem Rüstungsbereich, müssen jedoch der Proxy-Funktion der ökonomischen Spionage zugerechnet werden.

zur Verhinderung wirtschaftlicher Cyberspionage aus 2015 verantwortlich gewesen sein könnte. Inwiefern diese Annahme plausibel erscheint und welche weiteren, stärker innerchinesischen Faktoren ebenfalls einen Einfluss auf diesen zumindest scheinbaren Rückgang chinesischer US-Spionage im Jahr 2016 gehabt haben könnten, wird ebenfalls Gegenstand der Untersuchung der UV sein.[24]

Ein besonders vielschichtiger Fall, der nach seinem Bekanntwerden 2010 zu erheblichen politischen Spannungen zwischen den USA und China führte, war die sog. Spionageoperation ›Aurora‹. Diese war mutmaßlich von 2009 bis 2010 aktiv und nutzte einen Zero-Day-Exploit des Internet Explorers von Microsoft, um sich Zugang zu Googles sowie u.a. Adobes Netzwerken zu verschaffen (Naraine 2010). Über die Infiltration des Google-Service Gmail erlangten die Hacker zudem laut Medienberichten Informationen über in den USA operierende chinesische GeheimdienstagentInnen, die sich unter Überwachung der US-Behörden befanden (Nakashima 2013a). Weitere Ziele der als ›Supply-Chain-Attack‹ zu bezeichnenden Operation waren der chinesische Künstler und Dissident Ai Weiwei sowie wohl noch weitere chinakritische AktivistInnen im Ausland (Anderlini 2010). Die genaue Motivlage zur Initiierung dieser Spionageoperation wird bei der Analyse der UV von Interesse sein. Bemerkenswert ist jedoch bereits an dieser Stelle die Brisanz der Infiltration weltweit operierender US-Internetplattformen und Informationsdienste, die autokratischen Regimen Spionage und Überwachung auch außerhalb ihrer Informationssouveränitätssphäre in großem Stil erlaubt.

Mit insgesamt 26 Vorfällen stechen jedoch auch die Zivilgesellschaft,[25] EnduserInnen und Medien/JournalistInnen als Ziele domestischer Spionageoperationen Chinas heraus. Plausibel wird diese Annahme zusätzlich durch das verzeichnete Länderprofil der anvisierten Ziele: Fünfmal wurden AkteurInnen des Autonomiegebiets Tibet, viermal der autonomen Region Xinjiang, jeweils zwei Mal der VR China sowie Hongkong und einmal Taiwans zum Ziel. Dieses Akteursprofil deutet auf die intendierte Proxy-Funktion der Überwachung von RegimegegnerInnen oder Oppositionellen in der unmittelbaren Einflusssphäre des Landes hin, insbesondere in Gebieten mit entsprechenden Autonomie- und Sezessionsbestrebungen.[26] Ein weiteres Merkmal chinesischer Proxy-Operationen ist deren teilweiser Fokus auf Taiwan, was ebenfalls aus chinesischer

24 Für das Jahr 2016 berichtete Dell SecureWorks darüber hinaus von chinesischen Ransomware-Operationen, welche zuvor so nicht registriert wurden. Die Vermutung stand dabei im Raum, dass vor allem zuvor mit US-Spionage beauftragte Proxys in Folge des Abkommens zumindest für 2016 eine alternative Finanzierungsquelle benötigten und daher diesen Wechsel im Modus Operandi vollzogen BBC 2016. Ransomware-Operationen wurden im HD-CY.CON jedoch in erster Linie für nordkoreanische sowie russische AkteurInnen erfasst.

25 Ein Beispiel hierfür wären die Cyberoperationen gegen britische Think Tanks 2017, die laut CrowdStrike von chinesischen Hackern mit Verbindungen zur Regierung ausspioniert wurden, um an unveröffentlichte Informationen zu gelangen (Corera 2018).

26 2012 & 2013 gerieten jedoch auch zahlreiche US-Medienunternehmen und Zeitungen in das Visier chinesischer HackerInnen. Als Gründe hierfür wurde die Überwachung der Berichterstattung über China, sowie investigative Recherchen über den persönlichen Reichtum der Verwandten von Xi Jinping angeführt (Perlroth 2013). Dabei wurde jedoch nichts über Vergeltungsschläge im Cyberspace im Stile des Sony-Hacks 2014 durch Nordkorea bekannt. Vielmehr war für China wohl eher das Interesse nach möglichen weiteren Enthüllungen ausschlaggebend für die Infiltrationen.

Sicht im Sinne der Ein-China-Politik als domestische Überwachung, aus internationaler Perspektive dagegen als politische Spionage eines politischen Rivalen gedeutet werden muss.[27] In neun Fällen waren taiwanesische Entitäten unter den betroffenen Zielen, ein aktuelleres Beispiel hierfür sind die 2018 begonnenen und bis zumindest 2020 andauernden Kampagnen der Gruppierungen Taidoor und BlackTech, worin die taiwanesische Regierung das Ziel war (Lee 2020).[28]

Ein weiterer Strang chinesischer Cyberspionage gegen politische Ziele richtet sich auf den Konflikt um das Südchinesische Meer. So wurden vietnamesische und philippinische Ziele jeweils neunmal im HD-CY.CON für chinesische Proxy-Operationen verzeichnet,[29] wobei für letztere eine Episode, bestehend aus mehreren Einzelfällen, besonders interessant erscheint: Während einer Anhörung des ständigen Schiedsgerichts in Den Haag im Oktober 2015 kam es zu Cyberspionage mutmaßlich chinesischer HackerInnen, denen zumindest staatliche Verbindungen unterstellt wurden. Die Operation erlaubte es den AngreiferInnen, die vor allem aus Diplomatenkreisen stammenden, der Anhörung virtuell beisitzenden Personen zu hacken und so an deren für das Streitthema relevante Informationen und Kommunikation zu gelangen, möglicherweise auch, um im Falle eines Erfolges der Philippinen ähnliche Bestrebungen anderer Länder der Region bereits frühzeitig antizipieren zu können (Healey und Piiparinen 2015). Nachdem es im Juli 2016 schließlich zu einer Rüge Chinas seitens des Schiedsgerichts kam, wurden noch am selben Tag philippinische Regierungsbehörden in großer Zahl Opfer von DDoS- sowie Defacement-Angriffen, die mehrere Tage andauerten (Cimpanu 2016). In diesem Falle folgte die Attribution stärker dem Narrativ der patriotischen HackerInnen, denen eben nicht automatisch eine direkte Unterstützung oder Beauftragung der Regierung unterstellt werden kann. Nichtsdestotrotz erscheinen aufgrund der Kontrolle der KPC über den eigenen Informationsraum zumindest eine Duldung und wohl auch eine ideologische Unterstützung solcher Aktionen wahrscheinlich (›state-ignored‹ bis hin zu ›state-encouraged‹).[30] Komplettiert werden diese demselben konventionellem Konflikt zuzuordnenden Cyberoperationen durch zahlreiche großangelegte Spionagekampagnen, die bereits vor 2015 die Länder der Region hinsichtlich ihres privatwirtschaftlichen und politisch-militärischen Sektors zum Ziel hatten.

---

27 Auch wenn nur wenige Staaten Taiwan bislang offiziell als unabhängigen Staat anerkennen, unterstützen z.B. die USA aktuelle Bestrebungen Taiwans, Teil der UN zu werden und agieren zudem als eine Art militärische Schutzmacht ggü. Aggressionen der VR China.

28 Uiguren, Tibeter, Taiwanesen, chinesische DemokratieaktivistInnen sowie AnhängerInnen der Falun Gong werden auch als die »*Five Poisons*« Chinas bezeichnet (Hoffman und Mattis 2016).

29 Neben Taiwan wurden zudem als weitere Konfliktparteien in der Region fünfmal malaysische Ziele und zweimal AkteurInnen in Brunei anvisiert.

30 Die diese Operationen detektierenden IT-Unternehmen nahmen zum damaligen Zeitpunkt noch keine direkte Attribution in Richtung chinesischer Proxies vor, plausibilisierten jedoch sehr deutlich das chinesische Interesse an den dabei mutmaßlich erbeuteten Daten. Wie in vielen anderen Fällen auch, erfolgte darauf aufbauend trotzdem in den Kreisen politischer CybersicherheitsexpertInnen ein entsprechender Attributionslink, indem von einer »*Chinese Cyber Unit*« und nicht mehr nur von Cyberkriminellen wie zuvor im entsprechenden IT-Bericht gesprochen wurde (Piiparinen 2016).

Im HD-CY.CON wurde bereits für eine chinesische Proxyoperation aus dem Jahr 2003 ein zugrunde liegender konventioneller Konflikt registriert. Dabei handelte es sich um eine Spionageoperation gegen politische und kommerzielle Ziele in Taiwan. Ab 2015 kamen vor allem Cyberoperationen im Rahmen des bereits angesprochenen Regionalkonfliktes mit Ländern wie Vietnam, den Philippinen, Thailand sowie Japan im (Süd-)chinesischen Meer hinzu. Auch der Konflikt um das Autonomiegebiet Tibet verzeichnete affiliierte chinesische Cyberoperationen im HD-CY.CON, gleiches gilt für die Autonomiekonflikte mit Hongkong und der Mongolei. Der Konflikt zwischen China und Hongkong wurde vor allem ab 2016 im HIIK-Barometer als gewaltsam eingeordnet, der Konflikt mit der Mongolei bereits zuvor. Zudem wurden viele der zahlreichen chinesischen Spionageoperationen gegen US-Ziele dem im HIIK-Konfliktbarometer als niedrigschwellige Auseinandersetzung um ›International Power‹ deklarierten Konflikt zugesprochen.

Dass es sich bei den beschriebenen Fällen nahezu ausschließlich um Cyberspionage-Operationen handelte, spricht vor allem für die im Rahmen von (gewaltsamen) konventionellen Konflikten bedeutsame militärtechnologische Spionage als Proxy-Funktion. Die ›strategisch-operative Unterstützung gewaltsamer konventioneller Konflikte‹ könnte ebenfalls das Ziel gewesen sein, jedoch weniger im Sinne direkter, operativer Vorbereitungsmaßnahmen im Vorfeld konventioneller Militärschläge, wie sie für Russland im zweiten Fallbeispiel noch von Relevanz sein werden. Stattdessen wäre strategische Unterstützung hier als Informationsaufbau und -gewinn über die Kapazitäten und Handlungen des Gegners zu verstehen und nicht etwa als Cybersabotageakt, um den konventionellen Streitkräften ihre Arbeit direkt zu erleichtern.

Eine weitere Konfliktdyade, die zumindest außerhalb des vom HD-CY.CON erfassten Zeitraumes in die disruptiv konnotierten Proxy-Funktionskategorien im Rahmen gewaltsamer konventioneller Konflikte fallen könnte, ist China vs. Indien ab 2020. In diesem Jahr kam es zwischen den beiden Ländern zu militärischen Auseinandersetzungen im Himalaya-Gebirge. In der Folge fand im Oktober 2020 in der indischen Metropole Mumbai ein weitflächiger Stromausfall statt, für den untersucht wurde, ob eine Cyberoperation verantwortlich war. Nationale Medien verwiesen zeitgleich auf in der Vergangenheit identifizierte, chinesische Cyberoperationen gegen indische Ziele, wodurch China als möglicher Verantwortlicher suggeriert wurde (Joshi 2020). Diese These fachte ein Bericht des IT-Unternehmens Recorded Future im Februar 2021 weiter an: Darin wurde von beobachteten Malware-Infizierungen indischer Energienetzwerke seitens eines mutmaßlich chinesischen Proxys (»*RedEcho*«) berichtet (Insikt Group 2021a). Auch wenn Recorded Future selbst keine Aussage darüber treffen wollte, ob diese Malware-Implantate zu besagtem Stromausfall geführt haben, könnte bereits der bloße Verdacht einen potenziell intendierten Signaling- bzw. Abschreckungseffekt in Richtung Indien bewirkt haben. Diese Episode könnte darauf hindeuten, dass die im eigentlichen Untersuchungszeitraum nicht festgestellte, disruptive Form der strategischen Konfliktunterstützung bzw. -Schwächung politischer Gegner erst seit den letzten Jahren und in Zukunft noch häufiger von China bedient werden könnte.

Als weitere Proxy-Funktion könnte auch die Spionage/Unterminierung internationaler Organisationen künftig stärkere Relevanz für China erhalten. Im HD-CY.CON sind supranationale/internationale Organisationen als Ziele chinesischer Proxyoperationen

eher unterrepräsentiert. Das (noch) nicht im HD-CY.CON erfasste Beispiel der Spionageoperation gegenüber der Afrikanischen Union, die Ende 2020 bekannt und der chinesischen Proxy-Gruppe »*Bronze President*« zugesprochen wurde (Satter 2020), könnte als Indiz hierfür gewertet werden.

Die Häufigkeit der kritischen Infrastrukturen unter den chinesischen Proxyoperationen gilt es auszudifferenzieren, da dies eher eine Beurteilung der hiermit verbundenen Funktionen möglich macht (Abbildung 28).

Abbildung 28: Kritische Infrastrukturen als Ziele chinesischer Cyberproxyoperationen

(Eigene Darstellung auf Basis des HD-CY.CON)

Die Verteilung der Unterkategorien legt nahe, dass militärtechnologische Cyberspionage eine erklärungskräftige Cyberproxyfunktion für China darstellt. So wurden 2020 im Rahmen einer US-Anklage entsprechende Cyberspionageoperationen im Zeitraum zwischen 2009 und 2020 bekannt.[31] Dabei hackten zwei chinesische Bürger unter Anleitung und Hilfe eines MSS-Offiziers zahlreiche Verteidigungs-, Technologie, Software-, Gesundheitsforschungs- sowie Gamingunternehmen in Ländern wie den USA, Australien, Belgien, Großbritannien, Deutschland, Japan, Südkorea, Schweden, Spanien, Niederlande sowie Litauen. In der Anklageschrift wurde zudem auf den 2020 verstärkten Fokus der Spionage auf Biotechnologie-Unternehmen mit besonderer Relevanz für die Erforschung und Herstellung von Impfstoffen verwiesen (DoJ 2020d). Auch wenn dieser Teil der Operationen außerhalb des eigentlichen Untersuchungszeitraums liegt, verdeutlicht er die chinesische Nutzung von Proxys zur Anvisierung unterschiedlicher Sektoren über viele Jahre hinweg, deren Zielportfolio anscheinend relativ flexibel an die Erfordernisse des Regimes angepasst wird.

Cyberspionage im Rahmen der Covid-19-Pandemie wurde nicht nur China, sondern auch Russland, Nordkorea sowie dem Iran unterstellt (Macias 2020). Alle vier ›üblichen autokratischen Cyberverdächtigen‹ nutzten demnach ihre Cyberpotenziale zur Beantwortung der Pandemie. Diese Strategie lässt sich an der Schnittstelle zwischen Cyberspionage aus Gründen der nationalen Sicherheit sowie ökonomisch motivierter Cyberspionage verorten, was somit auch für China gilt. Ferner könnte der Fall darauf hindeuten, dass chinesische Proxys regelmäßig in die Kategorie der Moonlighter fallen. So beschreibt die US-Anklageschrift, wie sich die zwei Hacker durch ihre Operationen oftmals auch einen eigenen, finanziellen Vorteil verschafften, in anderen Fällen jedoch wieder dem MSS-Offizier zuarbeiteten (DoJ 2020d). Gestützt wird diese Annahme durch FireEyes Bericht über die chinesische APT41 und deren Cyberspionage-Kampagne von 2013 bis 2019, während derer sich die als staatlich gesponsert attribuierte Gruppierung durch ihre Aktivitäten auch selbst bereicherte (Fraser et al. 2019).

Die chinesische Cyberspionage um den US-Kampfjet F-35 des Unternehmens Lockheed Martin ist für diese Proxyfunktion ein weiteres Beispiel. Dessen Konstruktionspläne wurden von der chinesischen APT1 (aka Comment Crew/Byzantine Candor) bereits 2007 gehackt, in der Folge ähnelte der chinesische Kampfjet J-31 dem F-35 in erheblichem Maße (Gady 2015). Das US-Unternehmen Mandiant identifizierte APT1 im Rahmen seines Threat-Reports 2013 jedoch als PLA Unit 61398, weshalb der Fall und auch nahezu alle weiteren APT1-Operationen in die Kategorie der allgemein/direktstaatlich attribuierten Operationen fallen, entsprechend der vorgenommenen Attributionen (MANDIANT 2013).[32] Ein weiterer Fall militärtechnologischer Cyberspionage war die Infiltration dreier israelischer Rüstungskonzerne 2011. Für den Hack der am israelischen Raketen-

31 Im Datensatz wird diese Kampagne durch sechs Teiloperationen erfasst, da sie sich entsprechend der in der Anklage benannten Ziele zeitlich ausdifferenzieren lassen. Für die meisten Cyberkampagnen ist dies jedoch aufgrund der Darstellungsweise der Quellen nicht möglich.

32 Eine Ausnahme hiervon stellte ein Spionagefall dar, der Ende Februar 2013 APT1 zugerechnet, in besagter Attributionsquelle jedoch lediglich als mit der PLA affiliiert bezeichnet wurde (Clayton 2013).

abwehrsystem Iron Dome beteiligten Unternehmen wurde ebenfalls APT1 aka Comment Crew verantwortlich gemacht (Krebs 2014).

Die mehrfach unter den Zielen chinesischer Proxyoperationen vertretenen Telekommunikationsanbieter stellen dagegen für unterschiedliche Ziele attraktive Spionageziele dar: Zum einen können diese selbst anvisiert worden sein, zum anderen könnten aber auch bestimmte KundInnen dieser Anbieter im Sinne eines Supply-Chain-Hacks die eigentlichen Ziele gewesen sein. Dies betrifft andere Unternehmen[33] und politische/staatliche AkteurInnen genauso wie auch Teile der Zivilgesellschaft, z.B. im Ausland befindliche DissidentInnen. Dass chinesische HackerInnen die Vorzüge besagter Supply-Chain-Hacks weithin erkannt haben, belegte nicht zuletzt der Microsoft-Exchange-Hack, den das Unternehmen der von China gesponserten Hackergruppe »*Hafnium*« 2021 zuordnete (Microsoft Security 2021).

Tabelle 12 fasst die in diesem Kapitel herausgearbeiteten, dominanten Funktionen chinesischer Cyberproxys entsprechend ihrer Erklärungskraft zusammen.

Tabelle 12: Ausprägung der AV I auf Grundlage des HD-CY.CON für China

Starke Ausprägung	Mittlere Ausprägung	Schwache Ausprägung
Politische Cyberspionage (Beispiele: Belgien-State-Department-Hack 2008, OPM-Hack 2015)	Strategische Unterstützung gewaltsamer konventioneller Konflikte (Beispiele: Red-Alpha-Kampagnen, APT3-Spionage vs. Hongkong 2016)**	Schwächung politischer Gegner (Staaten) ohne gewaltsamen konventionellen Konflikt (Beispiel: Hacks während der kambodschanischen Wahlen 2018)
Ökonomische Cyberspionage (Beispiele: Operation Aurora 2009, MSS-Spionageoperationen des US-Indictments 2020)		Schwächung demokratischer Institutionen/Werte (Beispiele: New-York-Times-Hack)***
Militärtechnologische Cyberspionage (Beispiele: Byzantine Hades 2007, Iron-Dome-Hack 2011)		
Überwachung von RegimegegnerInnen (In- und Ausland) (Beispiele: Spionageoperationen gegen Uiguren und Tibeter)		

(Eigene Darstellung auf Basis des HD-CY.CON)
**Erklärungskraft im Sinne von Cyberspionage und weniger der Sabotage/Disruption.
***Erklärungskraft im Sinne von Cyberspionage und weniger des informationsbasierten Doxings.

33 Ein Beispiel hierfür ist vermutlich die Cyberspionage-Kampagne der chinesischen APT10 aka MenuPass/Stone Panda von 2016–2017 gegen indische, japanische und nordeuropäische Produktionsunternehmen (FireEye 2017), sowie auch die bekannte Operation »*Cloud Hopper*« gegen Managed Service Provider (Barry und Volz 2019).

5.3.1.2 Die Art und Anbindung chinesischer Cyberproxys

Für die Analyse der AV II folgt nun eine qualitative Untersuchung der maßgeblichen chinesischen Proxy-Gruppierungen und ihrer Operationen. Aufgrund der jedoch oftmals überlappenden und sich teilweise auch widersprechenden Designatoren der IT-Community werden die Gruppen entsprechend ihrer attribuierten Affiliationseinheiten auf staatlicher bzw. militärischer Seite gegliedert (Tabelle 13). Dabei werden auch Gruppierungen thematisiert, für die erst ab einem bestimmten Zeitpunkt keine Proxy-Attributionen, sondern seither direktstaatliche Attributionen vorgenommen wurden.

Tabelle 13: Institutionelle Affiliationen der im HD-CY.CON erfassten chinesischen Proxys[34]

PLA-affiliierte Gruppierungen	MSS-affiliierte Gruppierungen
APT1/Comment Crew/Byzantine Candor *(Unit 61398)*	Winnti Group *(Xicheng District, Peking)*
APT30/Naikon *(Unit 78020)*	APT3/Gothic Panda *(Boyusec)*
Tick *(Unit 61419)*	APT10/Cloud Hopper *(Tianjin State Security Bureau)*
Red Foxtrot *(Unit 69010)*	APT17/DeputyDog *(Jinan Bureau)*
Tonto Team/Cactus Pete *(Unit 65017)*	APT26/Turbine Panda *(Jiangsu Bureau)*
APT19/Deep Panda/Black Vine *(Unit unbekannt)*	APT40/Leviathan/Temp.Periscope *(Hainan State Security Department/Hainan Xiandu)*
	APT41 *(Chengdu 404 Network Technology)*

(Eigene Darstellung auf Basis des HD-CY.CON)

PLA

Nachfolgend werden die zentralen Erkenntnisse für chinesische APTs diskutiert, die entweder direkt der PLA angehören oder mit ihr zumindest in Verbindung stehen sollen. Dabei werden ihre operativen Ziele, ihr technisches Vorgehen im Hinblick auf die öffentlich bekannten Details ihrer Organisationsstruktur und teilweise ihre Akteurschaft analysiert.

34 Diese Tabelle erfasst ausschließlich jene chinesische APTs im HD-CY.CON, denen eine PLA- oder MSS-Affiliation bislang öffentlich zugesprochen wurde. Es existieren noch zahlreiche weitere chinesische Proxy-Gruppierungen, die vom HD-CY.CON erfasst werden, z.B. APT27/Emissary Panda, APT15/Mirage, APT20, APT31/Zirconium. APT2/Putter Panda (Unit 61486) wurde zudem in allen Fällen als allgemein/direktstaatlich attribuiert und ist daher kein Bestandteil der nachfolgenden Übersicht. Darüber hinaus sind weitere chinesische Proxy-Gruppierungen noch nicht im HD-CY.CON erfasst worden, wie etwa die für den Microsoft-Exchange-Hack verantwortlich gemachte HAFNIUM-Gruppierung (Microsoft Threat Intelligence Center 2021) oder auch die von Recorded Future 2020 identifizierte Gruppe TAG-22 (Insikt Group 2021c).

Bereits 2011 wurden durch die Veröffentlichung geheimer Diplomatenberichte der USA durch Wikileaks Details über die Zusammenarbeit zwischen der PLA und nichtstaatlichen HackerInnen bekannt. So wurde darin beschrieben, wie u.a. das chinesische Unternehmen TOPSEC, damals Chinas größter Anbieter von Produkten im Bereich der Informationssicherheit, durch die PLA finanziert wurde und in deren Auftrag HackerInnen aus dem zivilgesellschaftlichen Bereich engagierte (The New York Times 2009). Diese stammten auch aus der in IT-Kreisen bekannten »*Honker Union*«, einer Gruppierung selbsternannter patriotischer HackerInnen, die Anfang der 2000er Jahre im Rahmen des »*Sino-US-Cyber-War*« auf sich aufmerksam gemacht hatte (Tang 2001). TOPSEC begann dabei als kleine Forschungseinrichtung und entwickelte sich unter Anleitung und finanzieller Unterstützung der PLA zu einem Technologieunternehmen, das Teil des »*China Information Technology Security Center*« (CNITSEC) wurde (The New York Times 2009). Das CNITSEC ist eine mit der Evaluation der Sicherheit von Systemen der Informationssicherheit beauftragte, durch die Regierung mandatierte Institution. Interessanterweise schloss dieses bereits 2003 ein Information-Sharing-Abkommen mit Microsoft, durch das es (und damit auch TOPSEC) privilegierten Zugang/Informationen zu dessen Quellcode erhielt, um die chinesische IT-Infrastruktur besser schützen zu können. Die Tatsache, dass TOPSEC laut dem Diplomatenbericht bereits vor 2009 HackerInnen im Auftrag der PLA engagierte, lässt Zweifel daran aufkommen, dass TOPSEC tatsächlich »*in der Lage* [ist; Anm. d. Autorin], *geistiges Eigentum und vertrauliche Informationen angemessen zu schützen*«, wie es von Microsoft noch im Jahr 2019 als eine Bedingung für die Teilnahme an diesem Kooperationsabkommen formuliert wurde (»*Microsoft Government Security Program*« (GSP); Microsoft 2019). Das GSP könnte vor allem im Zuge des Microsoft-Exchange-Hacks 2021 in den verstärkten Fokus von Politik und Microsoft selbst geraten sein. Dies war zumindest für das rein kommerzielle Pendant, das »*Microsoft Active Protection Program*« (MAPP), offensichtlich der Fall, auch wenn eine Beendigung der Kooperation mit chinesischen Firmen aufgrund der Bedeutung des chinesischen Markts für Microsoft von Beobachtern als unwahrscheinlich eingestuft wurde (Mehrotra 2021).

Nachfolgend wird anhand der im HD-CY.CON erfassten PLA-Proxys analysiert, ob sich dieses Muster der Instrumentalisierung chinesischer Technologieunternehmen zur Anheuerung von HackerInnen auch für diese bestätigt.

APT1 (aka Comment Crew/Byzantine Candor)

Die bekannteste Hackergruppierung, die der PLA zugeordnet wird, ist die sog. APT1. Der HD-CY.CON erfasst für sie eine staatlich gesponserte sowie acht allgemein/direktstaatlich attribuierte Operationen. APT1 wurde bereits 2012 in IT-Community-Kreisen als staatlich unterstützt bezeichnet und u.a. für die im Datensatz verzeichnete Spionageoperation ›ShadyRat‹ verantwortlich gemacht. Dabei hatte die Gruppe zwischen 2006 und 2011 über 70 Ziele im Privat- und Unternehmenssektor sowie in Regierungskreisen weltweit ausspioniert. 2012 wurde im Zuge der Analyse der Operation festgestellt, dass APT1 mutmaßlich von Shanghai aus operieren würde (Clayton 2012), weiter reichte die Akteursidentifizierung an dieser Stelle jedoch (noch) nicht. Dies änderte sich mit dem für die private Threat-Research oftmals als wegweisend bezeichneten Bericht der IT-Firma Mandiant (heute zu Fireeye gehörend) aus dem Jahr 2013 mit dem Titel: »*APT1 – Exposing One of China's Cyber Espionage Units*« (MANDIANT 2013). In diesem Bericht identi-

fizierte Mandiant APT1 als »*People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department*«, besser bekannt als PLA Unit 61398. Als Evidenzen gab Mandiant u.a. die Lokalisierung der APT1 in bestimmten Teilen Shanghais, in denen die PLA stationiert ist, sowie deren mit besagter Unit übereinstimmende technische Vorgehensweisen an. In der Folge wurde die Gruppe auf Basis des Berichts zumeist mit der Unit gleichgesetzt (Sanger und Perlroth 2013). Drei Jahre zuvor hatte das Unternehmen noch konstatieren müssen: »*The Chinese government may authorize this activity, but there's no way to determine the extent of its involvement*« (MANDIANT 2010, S. 2). Auf 76 Seiten legt das US-Unternehmen dar, welche Informationen über APT1 respektive PLA Unit 61398 zusammengetragen und analysiert sowie welche Schlussfolgerungen gezogen wurden. So bestehe die Unit mutmaßlich aus mehreren Hunderten bis Tausenden MitarbeiterInnen,[35] die verantwortlich für die immense Masse an weltweit durchgeführten Cyberspionageoperationen vor allem gegen Unternehmen und Regierungen seien. Diese Dimensionen legen nahe, dass APT1/Unit 61398 für eine arbeitsteilige Durchführung der als persistent beschriebenen Cyberspionageoperationen in kleinere Arbeitseinheiten unterteilt ist. Auch die verwendete Angriffsinfrastruktur wurde als umfassend und geografisch expansiv beschrieben: »*937 Command and Control (C2) servers hosted on 849 distinct IP addresses in 13 countries*« (MANDIANT 2013, S. 3).

Der im Mandiant-Bericht herausgestellte Fokus der APT1 auf Wirtschaftssektoren in englischsprachigen Ländern, die im Rahmen des zwölften Fünf-Jahres-Plans der KPC als essenziell für Chinas Entwicklung identifiziert wurden, zeigt sich auch im HD-CY.CON. Die für APT1 kodierten Fälle weisen zum einen deutlichen US-Fokus auf, inkludieren zum anderen jedoch asiatische Industrieländer wie Japan und Südkorea. Interessant ist zudem, dass die erfassten Operationen zeitlich gesehen von 2006 bis 2015 andauerten.[36] Dass danach kein weiterer APT1-Fall mehr erfasst wurde, mag einer Lücke des Datensatzes oder der Konstruktion der Inklusionskriterien geschuldet sein. Alternative Erklärungen für das Verschwinden der Gruppe wären der Mandiant-Bericht sowie die 2014 nachgelagerte Anklage der USA.[37] Gleichzeitig deutet 2015 als letztes Endjahr einer APT1-Operation auf die in diesem Jahr begonnene Umstrukturierung und Reform der PLA hin.[38]

Der APT1-Bericht identifizierte auch zum ersten Mal nicht nur eine bestimmte staatliche Behörde und Unit als verantwortlich für die Tätigkeiten einer APT, sondern benannte auch deren Mitarbeiter. So sei für die APT1 u.a. ein Hacker mit dem Namen Wang Dong aka »*UglyGorilla*« aktiv gewesen, der Gegenstand der Anklage aus 2014 war. Aufgrund der Biografie der identifizierten Hacker, die bereits vor ihrer APT1-Zugehörigkeit

35 Wozu nicht nur HackerInnen, sondern auch sonstige IT-MitarbeiterInnen zählen.

36 2006 ist das Startjahr der frühesten Operation, 2015 das zuletzt erfasste Endjahr für APT1.

37 Die Implikationen dieser zunächst privatwirtschaftlichen und ein Jahr später politischen Attribution, in Form einer Anklage, werden im Rahmen der USA-Fallstudie genauer diskutiert.

38 Im Oktober 2018 wurde erstmals seit 2015 wieder im Rahmen einer Spionageoperation Quellcode gefunden, welcher mit der APT1 assoziiert wird. Das US-Unternehmen McAfee kam in ihrem Bericht jedoch zur Position, dass es sich dabei höchstwahrscheinlich eher nicht um die Rückkehr der Gruppe, sondern um einen anderen Akteur gehandelt haben müsse (Sherstobitoff und Malhotra 2018).

Hacking-Tätigkeiten nachgegangen sind, kann die Verantwortlichkeit der PLA gegenüber der APT1 mindestens als ›state-integrated‹ bezeichnet werden. Auf Grundlage dieser Erkenntnisse wurde die Gruppierung in der Folge auch nicht mehr als Proxy bezeichnet.

APT1 kann somit als eine Art Gründungsmythos chinesischer Spionageoperationen auf das geistige Eigentum hochmodernisierter Länder gesehen werden. Im zeitlichen Verlauf zeigt sich, dass die PLA in der Frühphase des Cyberkonfliktaustrages zwischen 2000 und 2010 hierbei eine dominante Rolle eingenommen hat. Bevor für das zivilgeheimdienstliche Pendant der Spionageeinheiten der PLA, das MSS, ebenfalls die diesem im HD-CY.CON zugesprochenen Proxy-Gruppierungen vorgestellt und hinsichtlich ihres Vorgehens sowie ihrer institutionellen Anbindung diskutiert werden, wird eine weitere mutmaßliche PLA-Gruppe thematisiert.

APT30 (aka Naikon/LotusPanda)

Eine weitere vom HD-CY.CON erfasste PLA-Gruppierung ist die APT30 mit zwei staatlich gesponserten Fällen und einem allgemein/direktstaatlich attribuierten Fall. Die Operationen der Gruppierung erstrecken sich von 2005 bis 2020 (Enddatum). Einer der beiden als staatlich gesponsert attribuierten Fälle (2005–2015) fügt sich in die von APT1 vorgegebene Aktivitätszeitleiste der PLA-Proxys ein. Dabei handelte es sich um eine weitangelegte Spionageoperation gegen ausländische Regierungen/Ministerien, Unternehmen sowie MedienvertreterInnen. Betroffen waren folgende Länder: Indien, Vietnam, Myanmar, Philippinen, Südkorea und Singapur. Im Kampagnen-Bericht beschreibt Fireeye das technisch-operative Vorgehen der Gruppierung folgendermaßen:

> »They prioritize their targets, most likely work in shifts in a collaborative environment, and build malware from a coherent development plan. Their missions focus on acquiring sensitive data from a variety of targets, which possibly include classified government networks and other networks inaccessible from a standard Internet connection. While APT30 is certainly not the only group to build functionality to infect air-gapped networks into their operations, they appear to have made this a consideration at the very beginning of their development efforts in 2005, significantly earlier than many other advanced groups we track.« (FireEye 2015a, S. 3)

Die Fähigkeit, auch ›Air-gapped Networks‹ zu infiltrieren, kann einerseits auf ein gewisses Maß an technischer Sophistiziertheit, andererseits auf die Instrumentalisierung eigener Spione oder umgedrehter InsiderInnen der besagten Zielsysteme hindeuten, wie es z.B. für Stuxnet diskutiert wurde. Laut CyberexpertInnen sei es zudem heute wesentlich einfacher, Steuerungsanlagen kritischer Infrastrukturen zu infizieren, da diese im Vergleich zu den Jahren 2000–2010 seltener mit Air-Gaps versehen seien (Muncaster 2019).

Bereits 2015 hatte das Unternehmen ThreatConnect einen eigenen Bericht über die APT »*Naikon*« veröffentlicht, die allgemein als mit APT30 übereinstimmend angesehen wird. In diesem Bericht ging ThreatConnect noch weiter als FireEye, indem das Unternehmen APT30/Naikon nicht nur als staatlich gesponsert bezeichnete, sondern das »*People's Liberation Army Chengdu Military Region (MR) Second Technical Reconnaissance Bureau (TRB)*«, bekannt auch als PLA Unit 78020, als Äquivalent auf der staatlichen Be-

hördenseite identifizierte (ThreatConnect 2015, S. 10). Auch im ThreatConnect-Bericht kommt der scheinbare Fokus der APT30 auf Ziele in der unmittelbaren Umgebung Chinas zum Ausdruck, vor allem im Bereich des Südchinesischen Meers, einer Region mit umkämpften Energierohstoffen. Wie im Falle des Mandiant-Berichtes über APT1, identifizierte ThreatConnect zudem namentlich einen mutmaßlichen Naikon/APT30-Hacker, dessen PLA-Anstellung u.a. durch seine akademischen Veröffentlichungen sichtbar wurde (ThreatConnect 2015, S. 10).

Tick

Im April 2021 wurde eine weitere chinesische APT erstmals offiziell mit der PLA in Verbindung gebracht: Tick (zwei Fälle im HD-CY.CON mit attribuierter staatlicher Unterstützung). So berichteten japanische Medien, dass deren Strafverfolgungsbehörden davon ausgingen, Tick »*has breached more than 200 Japanese companies and organizations since at least 2016*« (Cimpanu 2021b). Diese stammten besonders aus dem Unternehmens- und Forschungsbereich, genauer gesagt der Luftfahrt sowie Verteidigungsbranche. Dieses Angriffsprofil stimmt mit der identifizierten inhaltlichen Ausrichtung der PLA nach der Militärreform sowie der Errichtung der »*Strategic Support Forces*« (SSF) 2015 überein. Tick handele auf Geheiß der PLA Unit 61419, stationiert in Qingdao. Diese war laut Recorded Future bereits vor den Reformen 2015 für militärstrategische Spionage gegenüber Japan und Nordkorea verantwortlich (Cimpanu 2021b). Recorded Future fand im Mai 2021 zudem Evidenzen dafür, dass die Unit 61419 Antivirus-Software aus den USA, Europa und Russland gekauft hatte, mutmaßlich für eine realitätsgetreuere Testung der eigenen Cyberoperationen in eben jenen Ländern sowie zwecks eines Reverse Engineerings des Antivirus-Software-Codes, um diesen künftig effektiver umgehen zu können (Insikt Group 2021b).

RedFoxtrot

Ebenfalls erst im Juni 2021 identifizierte Recorded Future die staatlich gesponserte APT RedFoxtrot als Ableger der PLA Unit 69010 in Xinjiang und somit Teil der 2015 neu gegründeten SSF. Sie ist mit einem Fall im HD-CY.CON vertreten. Die folgenden Ausführungen des Berichtes belegen den vor allem geopolitisch-militärischen Fokus der Spionageoperationen, der sich in die strategische Neuausrichtung der PLA im Cyberspace ab 2015 einfügt:

> »RedFoxtrot has been active since at least 2014 and predominantly targets government, defense, and telecommunications sectors across Central Asia, India, and Pakistan, aligning with the likely operational remit of Unit 69010. Of particular note, within the past 6 months, Insikt Group detected RedFoxtrot network intrusions targeting 3 Indian aerospace and defense contractors; major telecommunications providers in Afghanistan, India, Kazakhstan, and Pakistan; and multiple government agencies across the region.« (Insikt Group 2021d)

Vor ihrer Integration in die SSF war die Unit bekannt als das ›Lanzhou Military Region's Second Technical Reconnaissance Bureau‹. Geholfen hatten den Analysten Defizite in der ›Operational Security‹ der Gruppierung, die es ihnen erlaubten, ihre Aktivitäten zur physischen Adresse in Xinjiang zurückzuführen (Insikt Group 2021d).

Der inhaltliche Fokus der hier behandelten PLA-Proxys war vor 2014/2015 somit auf kommerzielle Ziele vor allem in den USA sowie im südostasiatischen Raum gerichtet. Dabei wurden in mehrjährigen und arbeitsteiligen Kampagnen sensible Daten der Opfer in für Chinas Entwicklungsziele kritischen Bereichen gestohlen. Die Handlungen von Tick und RedFoxtrot reflektieren dagegen den militärisch-geopolitischen Fokus der PLA-Proxys ab 2015.

Auch wenn sich für APT1 und APT30 nicht die in den US-Diplomatenberichten beschriebene Nutzung technologischer Frontunternehmen seitens der PLA bestätigen lässt, unterstreicht gerade die APT1 die Inkorporierung zumindest anfänglich nichtstaatlicher Hacker in staatliche Institutionen und zum Zwecke offensiver Cyberoperationen.[39] Der Grad an staatlicher Kontrolle und Anleitung wird aufseiten der PLA-Gruppierungen als relativ hoch beschrieben, so ist für diese oftmals von mindestens ›state-integrated‹-Operationen auszugehen, wenn nicht gar ›state-executed‹, was einer Proxy-Attribution (z.B. für APT1) zunehmend die Grundlage entzog.

MSS

Das MSS ist der zivile Geheimdienstakteur Chinas, dem neben der PLA der größte Aktionsradius im Cyberspace attestiert wird. Es wurde 1983 gegründet und soll in erster Linie die staatliche Sicherheit schützen und AusländerInnen im Inland sowie potenzielle Bedrohungen sezessionistischer Bestrebungen überwachen. Durch die Gründung des MSS musste das *Ministry of Public Security* (MPS), eine Art Spiegelbehörde des MSS auf Polizei-Ebene, Kompetenzen im Bereich der Gegenspionage an das MSS abtreten (Mattis 2015a). Das Wappen des MSS ziert interessanterweise nicht das Emblem des chinesischen Staates, sonders das der KPC, deren Sicherung bei dessen Mandat letztlich im Vordergrund steht (vander Straeten 2020). Dem MSS wurde besonders in Folge der Umstrukturierung der PLA 2015 eine verstärkte und nun dominante Rolle im Rahmen der chinesischen Cyberspionage-Architektur attestiert (Lyngaas 2018).

Winnti (Umbrella) Group

Diversen chinesischen APTs werden Verbindungen zum MSS und dessen Agenten attestiert. Als eine Art Dachorganisation aufseiten der APTs kann die sog. ›Winnti Umbrella Group‹ gesehen werden, die als Sammelbegriff für APTs unter der Leitung des chinesischen Geheimdienstapparates verwendet wird.[40] Im HD-CY.CON wurden fünf Vorfälle in einem Zeitraum des jeweiligen Operationsbeginns von 2011 bis 2019 generisch Winnti zugesprochen. Dabei handelte es sich ausschließlich um Spionageakte, hauptsächlich gegen kommerzielle Ziele, aber auch gegen kritische Infrastrukturen (Gesundheits- und Chemiesektor). Neben deutschen sowie anderen weltweit verteilten Unternehmen zählten südkoreanische Firmen zu den betroffenen Akteuren, was das auf Wirtschaftsspionage ausgerichtete Portfolio der Winnti Gruppe verdeutlicht.

---

39 So war Wang Dong aka UglyGorilla vor seiner Hacking-Tätigkeit im Auftrag des Staates Mandiant zufolge ein an der Thematik der Cyber-Warfare interessierter Hacker (MANDIANT 2013, S. 52).

40 Synonym hierfür steht zudem der Name ›Axiom‹, der in einem Bericht des IT-Unternehmens Novetta die Operationen der ursprünglichen Winnti Gruppierung (Namensgebung durch Kaspersky 2013, s. Securelist 2013) beschrieb (Novetta 2014).

Die Winnti Gruppe wurde 2018 öffentlich erstmals als »*associated with the Chinese state intelligence apparatus, with at least some elements located in the Xicheng District of Beijing*« seitens eines Threat Intelligence-Berichtes bezeichnet (Hegel 2018, S. 3). Im Bericht wurde ferner auf die zahlreichen weiteren HackerInnengruppierungen verwiesen, die offensichtlich dieselben operativen und strategischen Ziele wie Winnti verfolgen und sich die dabei zur Anwendung kommenden Ressourcen teilen: »[…] *TTPs, infrastructure, and tooling show some overlap with other Chinese-speaking threat actors, suggesting that the Chinese Intelligence-Community shares human and technological resources across organizations*« (Hegel 2018, S. 5). Als zentrale Behörde innerhalb dieser ›Intelligence-Community‹ gilt das MSS. Eine personelle sowie materielle Ressourcenteilung zwischen einzelnen MSS-Proxys und MSS-Agenten spricht für eine einheitliche Struktur der Cyberoperationen, die auf ein gemeinsames Ziel ausgerichtet sind und deshalb oftmals auch arbeitsteilig zueinander agieren. Inwiefern sich dieser holistische Cyberansatz des MSS auch aufgrund der domestischen Interessen der Geheimdiensteliten plausibilisieren lässt, wird im weiteren Verlauf der Arbeit adressiert. Zusätzlich wird von Interesse sein, inwiefern das MSS auch in Abgrenzung zur PLA seit deren Umstrukturierung ökonomische Interessen Chinas zunehmend im Cyberspace verfolgt und wie sich dies durch die domestische Präferenzordnung erklären lässt.

Winnti-Operationen wurden grundlegend zwar als erfolgreich, gleichzeitig jedoch auch mit erheblichen Mängeln hinsichtlich ihrer ›Operational Security‹ beschrieben, wie sie etwa 2013 zur ›Überführung‹ der APT1 als eigentliche PLA Unit 61398 seitens Mandiant (u.a.) geführt hatten (Hegel 2018, S. 3; Soesanto 2020, S. 21). Eine weitere These besagt, dass es sich weniger um unbeabsichtigte Programmierfehler, sondern um bewusste Signaling-Effekte bezüglich der eigenen Unantastbarkeit handeln könnte (Tanriverdi et al. 2019). Der Aktionsradius von Winnti wird hinsichtlich ihrer präferierten Zielgruppe, führenden Wirtschafts- und Technologieunternehmen in vorrangig demokratischen Ländern, als extrem weitgehend bezeichnet. Deutschland steht hierbei besonders im Fokus, wie die Beispiele der Spionageoperationen gegen die Unternehmen Henkel, BASF, Siemens oder Roche belegen. Diese spezifische Anvisierung deutscher Unternehmen wurde 2019 auch in einem Bericht des deutschen Bundesamtes für Verfassungsschutz unterstrichen (BfV 2019).

APT17 (aka DeputyDog)

Als Teil der Winnti-Dachorganisation wird oftmals die APT17/DeputyDog bezeichnet. Der HD-CY.CON verzeichnet für diese Gruppierung fünf kodierte Cyberspionageoperationen, die sich, beginnend in 2009 u.a. gegen Regierungsbehörden, Unternehmen sowie JournalistInnen in den USA, Japan, Thailand, Südkorea und China selbst richteten und bis mindestens 2018 andauerten. 2013 wurden die Aktivitäten der Gruppierung durch eine Spionageoperation gegen japanische Organisationen erstmals durch FireEye bekannt gemacht (Moran und Villeneuve 2013). Besonderes Aufsehen erregte die bereits beschriebene Operation Aurora 2009, die in der Folge APT17 zugesprochen wurde. Das US-Unternehmen Symantec identifizierte die Aurora-Verantwortlichen jedoch als »*The Elderwood Group*«, auch bekannt unter dem Namen »*Beijing Group*«, die im Gegensatz zur APT17 bis dato mit der PLA in Verbindung gebracht worden war (Leyden 2013).

Zuvor hatte das Unternehmen Novetta, das DeputyDog entsprechend ihrer Namensgebung der Gruppierung Axiom zuordnet (Novetta 2014), deren technisches Vorgehen als recht variabel beschrieben: So wurde der Gruppierung im Rahmen einer einzigen Cyberoperation die Verwendung von vier verschiedenen Malware-Arten sowie neun Malware-Typen zugeschrieben, die von rudimentär bis sehr komplex bezeichnet wurden. 2014 wurde in demselben Bericht ein Novetta-Mitarbeiter zudem mit der Aussage zitiert, dass seiner Auffassung nach Axiom (aka APT17) Teil des chinesischen Geheimdienstapparates sei (Gertz 2014b).[41]

Im Jahr 2015 berichtete FireEye über die Verschleierungstaktiken der Gruppe hinsichtlich ihrer Command-and-Control-Server, um ein ausreichendes Maß an Persistenz der Operationen zu erreichen (FireEye 2015b). Defizite in der Operational Security können somit zwar Attributionslinks ermöglichen, müssen jedoch gleichzeitig nicht zu einer Beendigung der Operation führen. Über die institutionelle Anbindung von APT17 wurden schließlich im Juli 2019 Details bekannt. So berichtete die Gruppierung ›Intrusion Truth‹, dass APT17 in Wahrheit zu chinesischen Cybersicherheitsfirmen gehöre, die unter Anleitung eines zuvor als MSS-Agenten identifizierten Offiziers stünden (Intrusion Truth 2019a).[42] Diese Annahme wurde im Vorfeld über mehrere Blogeinträge plausibilisiert, indem am Anfang besagter MSS-Offizier in Jinan konkret benannt und mit Cyberoperationen in Verbindung gebracht wurde (Intrusion Truth 2019c). In einem nächsten Blogbeitrag belegte Intrusion Truth die Verbindung zwischen besagten Technologieunternehmen und dem MSS-Offizier. Darüber hinaus enthüllten sie, dass Hacker von APT17 mutmaßlich mit diesen Unternehmen assoziiert seien, und konnten letztlich die Annahme, dass APT17 durch das MSS angeleitet wird, sukzessive plausibilisieren (Intrusion Truth 2019a). An dieser Stelle wurde jedoch nicht eindeutig geklärt, ob die APT17-Hacker offizielle Mitarbeiter der Technologieunternehmen oder von diesen angeheuerte Subhacker sind. Zu APT17 fand das Attributionskollektiv ferner heraus, dass diese in der Vergangenheit nicht nur für das MSS tätig waren, sondern auch zum eigenen finanziellen Profit hackten (Intrusion Truth 2019b). Ob es sich hierbei jedoch um ›state-ignored‹- oder ›state-rogue-conducted‹-Cyberoperationen handelte, kann an dieser Stelle nicht beurteilt werden. Im Gegensatz zu den beschriebenen, in staatliche PLA-Einheiten integrierten Gruppierungen trifft für die Operationen der APT17 als MSS-Proxy jedoch aufgrund der Zugehörigkeit zu offiziell privaten Technologieunternehmen die Bewertung ›state-coordinated-/state-ordered‹ zu.

APT3 (aka Gothic Panda)

Als weiterer MSS-Proxy ist die APT3 mit fünf erfassten Proxy-Operationen von 2011 (Startjahr der ersten Operation) bis 2018 (zuletzt verzeichnetes Endjahr) im HD-CY.CON

41 Ob es sich dabei also gar nicht um eine Proxy-Gruppe, sondern schon um einen direktstaatlichen Akteur handeln könnte, wurde an dieser Stelle somit noch nicht beantwortet.

42 Der genaue Hintergrund des selbsternannten Attributionskollektivs ist bis dato nicht bekannt. Aufgrund des starken Fokus auf die Entlarvung chinesischer Staatshacker seit der Gründung der Gruppe 2017, erscheint ein US-Hintergrund jedoch nicht unplausibel zu sein. Hinzu kommt, dass Intrusion Truth aufgrund ihrer Anonymität chinesische Individuen auch konkret benennen kann, wovor IT-Unternehmen zurückschrecken, da sie dies anfällig für mögliche Verleumdungsklagen machen würde (Cox 2018).

vertreten. Sie war die erste chinesische Hackergruppierung, die das Attributionskollektiv Intrusion Truth 2017 als kommerziellen Proxy (IT-Unternehmen mit dem Namen Boyusec) des MSS identifizierte (Intrusion Truth 2017). Eine Woche später bestätigte dies auch das IT-Unternehmen Recorded Future (Insikt Group 2017b).

Wie später auch für APT17, baute Intrusion Truth seine Attributionsbeweisführung sequenziell auf: Zunächst wurden Individuen mit den Cyberoperationen von APT17 in Verbindung gebracht, diese dann als Anteilseigner von Boyusec identifiziert und die Erkenntnisse letztlich mit der bereits 2016 veröffentlichten Rolle des Unternehmens als MSS-Vertragsnehmer in Beziehung gesetzt (Gertz 2016b). Im 2016 bekannt gewordenen Pentagon-Bericht wurde Boyusec nicht nur als Frontorganisation für das MSS bezeichnet, sondern auch als Kooperationspartner des Technologieunternehmens Huawei, das nicht zuletzt im Rahmen der weltweiten Debatte um dessen Beteiligung am Aufbau nationaler 5-G-Netze im Fokus stand. Laut dem Pentagon-Bericht arbeiteten Boyusec und Huawei damals gemeinsam an Sicherheitsprodukten, die »*will allow Chinese intelligence to capture data and control computer and telecommunications equipment*« (Gertz 2016b). Das MSS könnte somit für Hackingoperationen auf ausländische Ziele die eher unbekanntere, inländisch konzentrierte Firma Boyusec nutzen, um die stärker global ausgerichteten Marktambitionen Huaweis hierdurch nicht zu gefährden. Das Ausmaß staatlicher Verantwortlichkeit kann hier wie für APT17 stärker als ›state-coordinated/state-ordered‹ bezeichnet werden.

Bemerkenswert ist im Falle der APT3-Attribution durch Intrusion Truth zudem, dass das US DoJ sechs Monate nach der Identifizierung von APT3 als Boyusec und somit mutmaßlichem Cyberproxy Chinas Anklage gegen Mitarbeiter von Boyusec wegen Computer-Hackings und anderen Straftaten erhob. Die Taten richteten sich u.a. gegen Siemens und Moody's Analytics, die Angeklagten wurden jedoch nicht als Proxys bezeichnet (Cox 2018). Die Webseite von APT3 war nach dem Blogpost von Intrusion Truth bereits am darauffolgenden Morgen nicht mehr online, seither wurde keine Aktivität der Gruppierung mehr festgestellt (Intrusion Truth 2018b). Beobachter schlussfolgerten, dass die Gruppierung aufgrund ihres ›Naming-and-Shaming‹ sowie der damit verbundenen Anklage aufgelöst wurde (Chin 2017).

Der HD-CY.CON erfasst fünf Operationen der APT3. Dabei wurden Länder wie die USA, Belgien, Deutschland, die Philippinen, Vietnam sowie Ziele in Hongkong ausspioniert. Konkret visierten die HackerInnen Teile kritischer Infrastrukturen, Unternehmen sowie in einem Fall die Regierung Hongkongs an.[43] IT-Unternehmen attestierten APT3 ein ab 2015 gewandeltes Zielprofil weg von US-AkteurInnen und stärker hin zu Zielen in Hongkong. Diese Beobachtung wird durch die im HD-CY.CON erfassten Vorfälle gestützt. Das technische Vorgehen der APT3 beschrieb Recorded Future als sophistiziert. Die Gruppe »*utilizes a broad range of tools and techniques including spearphishing attacks, zero-day exploits, and numerous unique and publicly available remote access tools (RAT)*« (Insikt Group 2017b).

43 Eine weitere, in Bezug auf die strategisch-technische Sophistiziertheit der APT3 aufschlussreiche Episode ist deren berichtete Nutzung des NSA-Tools »*Eternal Romance*«, vor dessen Veröffentlichung durch die Gruppierung »*Shadow Brokers*«, was laut IT-Unternehmen Check Point ein »*Reverse Engineering*« des Tools seitens APT3 vermuten lässt (Vavra 2019).

APT10 (aka MenuPass, Stone Panda, Cloud Hopper)

Als weiteren MSS-Proxy benannte Intrusion Truth die APT10: Diese hatte zuvor durch Hacks mit globaler Reichweite, etwa auf Minengesellschaften, IT-Service-Provider sowie Unternehmen aus dem herstellenden Gewerbe in den USA, Großbritannien und Indien, auf sich aufmerksam gemacht. Ein zentrales Charakteristikum der Gruppe waren ihre häufigen Operationen gegen »*Managed-Service-Provider*« (MSP), um über deren Lieferkette an deren KundInnen heranzukommen (Cox 2018). Eine dieser Operationen, »*Cloud Hopper*«, wurde Gegenstand sowohl eine US-Anklage (2018c) als auch der erstmaligen Anwendung der »*Cyber Diplomacy Toolbox*« der EU 2020 (Bendiek und Schulze 2021).

Im August 2018 veröffentlichte Intrusion Truth in mehreren Blogposts stetig neue, aufeinander aufbauende Informationen zur Identität der APT10-Hacker, deren Assoziierung mit zwei chinesischen Technologieunternehmen und letztlich der Verbindung zwischen einem der APT10-Hacker und dem MSS (Intrusion Truth 2018a). Interessant hierbei war, dass sich das Kollektiv nicht nur auf öffentliche IT-Berichte sowie anderweitige Informationen aus dem Umfeld der englischsprachigen IT-Unternehmen oder Social-Media-Accounts identifizierter Hacker bezog, sondern auch den Uber-Beleg eines APT10-Hackers als Beweis anführte. Dieser belegte seine Fahrten in das Hauptquartier des ›Tianjin State Security Bureau‹, einem Regionalableger des MSS. Diese Form der Beweiserhebung erforderte aus Sicht anonym gebliebener CybersicherheitsexpertInnen das Hacken des Uber-Accounts oder der benutzten Uber-App (Cox 2018), was die Fähigkeiten sowie den Willen zur Anwendung offensiver Cyberfähigkeiten der Intrusion Truth-Gruppierung nahelegt.

Interessant ist im Zusammenhang mit APT10, dass auch diese nur wenige Monate nach Veröffentlichung des Intrusion Truth-Blogposts zum Gegenstand einer DoJ-Anklage wurde. Während in der APT3-Anklage das MSS bzw. dessen Regionalbüro keine Erwähnung fand, konstatierte die APT10-Anklage, die Gruppe »*acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau*« (DoJ 2018c). Darüber hinaus wurden über die Art der Beziehung zwischen MSS und APT10 jedoch keine weiteren Angaben gemacht, sodass eine Bewertung des Verantwortlichkeitsgrades, ob es sich um ›state-coordinated‹- oder sogar ›state-ordered‹-Operationen gehandelt hat, auf Grundlage dieser Informationen erschwert ist. Die laut Intrusion Truth jedoch gehäuften Fahrten des getrackten APT10-Hackers in das Büro des MSS in Tianjin lassen zumindest auf eine verstetigte Auftragsbeziehung schließen.

Der HD-CY.CON erfasst für APT10 sechs Fälle (Operationsstartjahre 2006–2019), in denen u.a. Telekommunikationsunternehmen mit globaler Streuung, Unternehmen, weitere Teile kritischer Infrastrukturen sowie in einem Falle auch eine Regierungsorganisation betroffen waren. Die betroffenen Entitäten verteilten sich hauptsächlich auf Europa, die USA, Südamerika sowie Asien (Japan/Indien).

APT40 (aka Leviathan/Temp.Periscope)

Als vierte durch Intrusion Truth als MSS-Proxy identifizierte Gruppierung erfasst der HD-CY.CON APT40 mit sechs Cyberoperationen (Startjahre 2011–2019). Diese sind dabei hinsichtlich des Länderprofils relativ konträr: So wurde 2017 das kambodschanische Wahlsystem in Teilen infiltriert, während 2018 ein britisches Ingenieursunternehmen ausspioniert wurde. Das Unternehmen FireEye konstatiert für APT40, dass dieses mut-

maßlich die Stärkung der chinesischen Seestreitkräfte durch entsprechend auf in diesem Bereich tätige Unternehmen ausgerichtete Spionageoperationen zum Ziel hat (Plan et al. 2019). Dies spiegelt sich im HD.CY-CON wider, da das Unternehmen aus Großbritannien auch im Bereich der maritimen Verteidigung tätig ist (Proofpoint 2017; Insikt Group 2018a).

Wie auch für APT3, attestierte die IT-Community der APT40 ein über die Zeit gewandeltes bzw. erweitertes Zielportfolio. So kamen ab 2017 neben dem maritimen Fokus auch Wahlsysteme asiatischer Länder hinzu. Zudem mutmaßte FireEye, dass das Vorgehen der Gruppe sich in Zukunft Erfordernissen der OBOR-Initiative anpassen könnte (Plan et al. 2019). Intrusion Truth identifizierte APT40 im Januar 2020 als das MSS-Frontunternehmen »*Hainan Xiandu*«, kontrolliert vom »*Hainan State Security Department*« (Intrusion Truth 2020). Bemerkenswert war hierbei abermals die intensive Nutzung von Informationen aus den Social-Media-Accounts der identifizierten Hacker. So war darin ein APT40-Mitglied in einer MSS-Uniform abgebildet und berichtete in einem Chat im Jahr 2009 über seine neue Tätigkeit für die Behörde (Intrusion Truth 2020). Die Art der Staat-Proxy-Beziehung kann entsprechend einer US-Anklage aus 2021 als ›state-ordered‹ bewertet werden: So belieferten die darin angeklagten MSS-Offiziere die APT40-Mitglieder mit Malware und ordneten zahlreiche Hackingoperationen selbst an (DoJ 2021, S. 12).

APT41

Mit einem Fall im Datensatz vertreten, stellt die APT41 einen weiteren chinesischen Cyberproxy dar, jedoch bislang ohne erfolgte PLA- oder MSS-Zuordnung. Eine US-Anklage aus 2020 spricht jedoch aus zwei Gründen eher für das MSS: Erstens wird hier APT41 mit Winnti in Beziehung gesetzt und zweitens wird beschrieben, wie APT41 aus einem Technologieunternehmen heraus agiert (»*Chengdu 404*«), was der beschriebenen Vorgehensweise des MSS entspricht (DoJ 2020b).

Wie das IT-Unternehmen FireEye im Jahr 2019 berichtete, zeichnet sich APT41 durch die Nutzung nichtöffentlicher Malware zum Zwecke der persönlichen Bereicherung aus, ein Alleinstellungsmerkmal im Gegensatz zu den anderen chinesischen APTs (Fraser et al. 2019). Besagter Bericht zur ›Moonlighting‹-Aktivität der APT41 wurde auch in den HD-CY.CON übernommen, allerdings mit dem Startjahr 2013, da laut FireEye im eigentlichen Startjahr 2012 ausschließlich Videospielhersteller zur persönlichen Bereicherung anvisiert wurden, was somit noch keinen Teil der eigentlichen Proxy-Tätigkeit darstellt. Im weiteren Verlauf wurden unterschiedliche Unternehmen und Organisationen aus dem Technologiebereich sowie Sektoren kritischer Infrastrukturen ausspioniert. FireEye teilte an dieser Stelle die oft getätigte Annahme, dass sich das Täterprofil von APT41, wie das anderer Gruppierungen auch, direkt aus den Erfordernissen der veröffentlichten Fünfjahrespläne der KPC ergäbe (Fraser et al. 2019).

Der offensichtlich dualistische Charakter der APT41 indiziert ein gewisses Maß an Schutz bzw. zumindest Duldung seitens der GeheimdienstakteurInnen gegenüber diesen kriminellen Operationen, mutmaßlich solange sie sich nicht gegen chinesische Unternehmen und AkteurInnen richten (›state-ignored‹). In einer 2020 veröffentlichten US-Anklageschrift bekräftigen die darin angeklagten APT41-Hacker diese Annahme selbst. So wurden Gespräche zwischen den Hackern überliefert, in denen sie ihr Verhältnis zum MSS wie folgt beschrieben (Auszug aus der Anklageschrift):

»JIANG and his associate agreed that JIANG's working relationship with the Ministry of State Security provided JIANG protection, because that type of association with the Ministry of State Security provided such protection, including from the Ministry of Public Security, ´unless something very big happens.« (DoJ 2020b, S. 6)[44]

Es stellt sich somit die Frage, ob die seitens FireEye berichtete Moonlighting-Kampagne von APT41 unter Duldung des Staates ein Einzelfall oder Hinweis auf eine weitere Verbreitung dieser Praxis auf chinesischem Boden ist. Eine an dieser Stelle (spekulative) These könnte besagen, dass, entsprechend der im FireEye-Bericht aufgezeigten Zeitleiste der anvisierten Ziele, APT41 durch ihre anfangs ausschließlich auf den eigenen Profit ausgerichteten Operationen staatliche Behörden auf sich aufmerksam gemacht haben könnte. In der Folge könnte es zur Aufnahme der Proxy-Tätigkeit gekommen sein, um weiterhin auch den eigenen Geschäften nachgehen zu können (Wandel von ›state-rogue-conducted‹ zu ›state-ignored‹ und ›state-ordered‹-Operationen).

»An APT with no name«[45]

Zum berichteten Moonlighting von APT41 passt die US-Anklageerhebung gegen zwei chinesische Hacker aus 2020, denen ähnliche Aktivitäten angelastet wurden. Diese wurden von John C. Demers, dem Leiter der Justice Department's National Security Division, wie folgt kommentiert:[46]

»*China has now taken its place, alongside Russia, Iran and North Korea, in that shameful club of nations that provide a safe haven for cybercriminals* in exchange for those criminals being ›on call‹ to work for the benefit of the state, here to feed the Chinese Communist Party's insatiable hunger for American and other non-Chinese companies' hard-earned intellectual property, including covid-19 research.« (Zitiert in Marks 2020)

Die Anklage stellte die erste dar, in der chinesische Hacker sowohl für private als auch staatlich gesponserte Operationen verantwortlich gemacht wurden. Das Zitat von Demers könnte darauf hindeuten, dass die USA dieses Moonlighting entgegen der oben getätigten Überlegungen tatsächlich als eine erst seit kurzem entwickelte, chinesische Praxis ansehen und zuvor von einer klareren Trennung zwischen domestischen Cyberkriminellen und staatlichen AkteurInnen ausgegangen sind. Aufschlussreich ist die Anklageschrift auch deshalb, da hier direkt die materielle Form der Unterstützung des benannten MSS-Offiziers für die Hacker beschrieben wird, ähnlich wie in der Anklage gegen

44 Das chinesische Unternehmen, für das die APT41-Hacker arbeiten, brüstete sich auf seiner Webseite offen mit seiner patriotischen Gesinnung und dass staatliche und militärische AkteurInnen zu dessen Kunden zählten (DoJ 2020b, S. 3). Diese Angaben können zweifelsohne als ein Mangel an Operational Security, jedoch weniger auf der technischen Ebene gesehen werden.

45 Dies ist der Teilüberschrift des Intrusion Truth-Blogeintrags zur Identität der nachfolgend behandelten Hacker entlehnt (Intrusion Truth 2021).

46 Die im Indictment gelisteten Hacking-Operationen sind im HD-CY.CON in sechs Einzelvorfälle unterteilt, mit den Startjahren 2014 bis 2019. Da entsprechend der Anklage eine aktive Beteiligung des darin benannten »*MSS-Officer 1*« an den Hackingoperationen nicht ausgeschlossen werden kann, wurden diese alle als allgemein/direktstaatlich kodiert. Eine Kodierung der Fälle als staatlich gesponsert wäre jedoch ebenso zutreffend gewesen, da der MSS Offizier die Hacker u.a. mit Malware belieferte und diese zudem auch aus persönlichen Motiven hackten (DoJ 2020d).

APT40. Der Offizier habe die Hacker mit Zero-Day-Exploits versorgt, um das anvisierte Ziel, in diesem Fall eine burmesische Menschenrechtsgruppe, infiltrieren zu können (DoJ 2020d, S. 4). Dieses Vorgehen spricht für einen ›state-ordered‹-Fall, in dem ein Proxy zur finalen Ausführung einer Operation benutzt wurde, für die die staatliche Behörde selbst bereits die notwendigen technischen Tools besaß. Plausible Deniability kann somit als primäre Motivation der Proxy-Nutzung identifiziert werden.

Auch Intrusion Truth recherchierte über die beiden angeklagten Hacker sowie den nur als »*MSS Officer 1*« benannten Akteur. Im Gegensatz zu ihren bisherigen Enthüllungen taten sie dies jedoch erst nach der Veröffentlichung der Anklageschrift. Inwiefern sich dies in eine möglicherweise gewandelte Attributionspolitik der USA gefügt haben könnte, wird in der ersten demokratischen Fallstudie genauer diskutiert. Intrusion Truth fand dabei zum einen heraus, dass auch diese beiden Hacker über Frontunternehmen aktiv waren, und enthüllte zum anderen den Namen des MSS-Offiziers (Intrusion Truth 2021). Die beiden Hacker konnten diesmal jedoch keiner bereits in der IT-Community bekannten APT zugeordnet werden. Dass das DoJ – wie zuvor für APT 3 – das Guangdong State Security Department benannte, sollte an dieser Stelle nicht als hinreichender Beweis für eine mögliche APT3-Zugehörigkeit gewertet werden. Zweifelsohne ist die Anklage aus 2020 im Zuge der besonders gegen Biotechnologie-Unternehmen im Rahmen der Corona-Pandemie gerichteten Spionageoperationen die bislang detaillierteste des US DoJ.

Zusammenfassend werden dem MSS eine größere und gewissermaßen diffuser zu definierende Zahl an Proxys zugesprochen als der PLA. Das MSS verlässt sich somit noch stärker auf eine Vielzahl an unterschiedlichen AuftragnehmerInnen, die entsprechend der behandelten Beispiele insbesondere aus dem (quasi-)privatwirtschaftlichen Sektor kommen. Die betreffenden Technologieunternehmen wiesen dabei bislang jedoch einen überwiegend national orientierten Fokus auf, sodass international agierende Firmen wie Huawei durch offensive Cyberproxy-Operationen nicht noch stärker in den Fokus und unter den Druck westlicher Firmen gerieten.[47] Die MSS-Proxys übernahmen insbesondere ab 2015 den Bereich der Wirtschaftsspionage, wobei sich die unterschiedlichen APTs in Teilen auf unterschiedliche Sektoren und somit Adressaten fokussierten. Die Beispiele von APT3, APT10, APT17 und APT40 belegen eindeutig das ab 2015 prävalente Muster chinesischer Staat-Proxy-Nutzung im Sinne von ›state-integrated-/state-ordered‹-Operationen: Das Auslagern von Hacks an Frontunternehmen im Technologiebereich, zu deren Führungspersonen zumeist direkte, personelle Verbindungen seitens des MSS bestehen. Ein Großteil der im HD-CY.CON für diese APTs verzeichneten Operationen fand erst nach 2015 und damit nach der großangelegten Umstrukturierung der PLA (Errichtung der SSF) statt (Costello und McReynolds 2018). An dieser Stelle kann nicht beurteilt werden, ob die hier beschriebene Proxy-Nutzung über IT-Vertragsnehmer bereits vor dieser Umstrukturierung angewandt wurde. Denkbar ist auch, dass diese ein Produkt der gestiegenen Kompetenzen des Ministeriums im Bereich der Cyberspionage und somit

47 So ist für Software-basierte Operationen eine physische Stationierung der eigenen IT-Firmen im Ausland weniger notwendig, als im Falle Hardware-basierter Überwachung, wie sie Huawei im Zuge des 5G-Aufbaus unterstellt wurde (Ptak und Pawlak 2021).

einen Versuch der Risikominimierung für derartige Operationen darstellte. Aufschlussreich ist diese Vorgehensweise jedoch, da sie zeigt, dass chinesische StaatsakteurInnen auch heute noch trotz gestiegener eigener Kapazitäten den Umweg über Proxys nehmen, vermutlich, um den Attributions- und Verantwortungsnachweis zu erschweren. Ein Ziel könnte jedoch auch sein, hierdurch einen direkteren Zugriff auf die Technologieunternehmen und deren Cyberaktivitäten zu erlangen.

Mitverantwortlich für die größere Anzahl an berichteten MSS-Proxys könnte jedoch auch deren stärkerer Aktionsradius ab 2015 und damit in einer Zeit sein, in der die privatwirtschaftliche Threat-Research-Analysis bereits weitaus stärker entwickelt war als zwischen 2000 und 2005. Gegen diese These sprechen die 2021 getätigten PLA-Attributionen der APTs Tick und RedFoxtrot, die auch auf militärischer Seite ein gewisses Spektrum an unterschiedlichen Proxys andeuten, nunmehr auch oder vor allem im Rahmen von konventionellen Konflikten. Bemerkenswert ist zudem, dass der APT17/DeputyDog in IT-Kreisen zumindest in der Vergangenheit Verbindungen zur Elderwood Group/Beijing Group unterstellt wurden. Das heißt, es wurden Verbindungen zwischen einer MSS-affiliierten und einer PLA-affiliierten Gruppierung konstruiert (Leyden 2013). Auf operativer Ebene scheinen daher gewisse Kooperationsformen zwischen den beiden Seiten zu existieren.

Für die chinesische Cyberproxy-Nutzung spielten zu Beginn somit noch stärker zivilpatriotische HackerInnen unter Anleitung der PLA bzw. nach Integration in deren Einheiten eine Rolle (›state-integrated/state-executed‹), wurden in der Folge jedoch vor allem unter MSS-Direktive zunehmend durch kommerzielle Proxys abgelöst (›state-coordinated/state-ordered‹) (vgl. Boeke und Broeders 2018, S. 83).[48]

Als Abschluss der Analyse der AV II wird nun eine weitere für die Arbeit interessante chinesische APT vorgestellt:

RedAlpha

Die chinesische Proxygruppe Red Alpha ist erst 2018 in Erscheinung getreten und wurde im HD-CY.CON in drei Fällen als verantwortlich attribuiert (Startjahre 2016–2018). RedAlpha verwendete laut Recorded Future im Rahmen zweier Spionagekampagnen gegen die tibetische Gemeinschaft bei einer registrierten Domain einen Begriff, der sich als »*The Chinese People's Liberation Army*« übersetzen lässt (Insikt Group 2018b). Recorded Future mutmaßte, dass dies entweder mangelnde Sorgfalt der Hacker oder eine bewusste False-Flag-Aktion zulasten der PLA gewesen sein könnte. In Verbindung mit der offensichtlich zeitlich koordinierten Ausnutzung von Sicherheitslücken in einem Zeitraum, in dem die »*Chinese National Vulnerability Database*« (CNNVD) absichtlich deren Veröffentlichung hinauszögerte (Insikt Group 2018b), könnte dies die Vermutung einer False-Flag-Operation, jedoch nicht von externen AkteurInnen sondern dem MSS, stärken. Zuvor hatte Recorded Future über den erheblichen Einfluss des MSS auf die Veröffentlichungspraxis der CNNVD berichtet, um die Sicherheitslücken vor ihrer Veröffentlichung gezielt ausnutzen zu können (Moriuchi und Ladd 2017). Weitere Unterstützung erhält die

---

48 Eine weitere Gruppierung, die dem MSS zugeordnet wird, ist Turbine Panda/APT26. Deren Verbindung zum Jiangsu Ministry of State Security (JSSD) wurde in einer 2018 veröffentlichten US-Anklageschrift umfangreich beschrieben (DoJ 2018a).

These der innerchinesischen Revierkämpfe durch die im Bericht getätigte Beobachtung, dass RedAlpha sich technischer Infrastrukturen bediente, die u.a. mit dem mutmaßlichen MSS-Proxy APT17/DeputyDog assoziiert werden.

Diese Ausführungen zeigen einmal mehr, welche Schwierigkeiten im technischen und darauf aufbauend politischen Attributionsprozess existieren und wie Staaten diese durch mehrfach verwendete Angriffsinfrastrukturen und Methoden vergrößern können. RedAlpha wird im Rahmen dieser Arbeit somit weder der PLA noch dem MSS zugeordnet.

5.3.2 Chinas Cyberakteursumwelt

In diesem Abschnitt wird untersucht, auf welche Weise Chinas Cyberakteursumwelt zu Beginn des Untersuchungszeitraums sowie im weiteren Verlauf ausgeprägt war. Somit kann bewertet werden, inwiefern die notwendigen Voraussetzungen für die festgestellte Proxy-Nutzung auf staatlicher, privatwirtschaftlicher, zivilgesellschaftlicher sowie krimineller Ebene vorhanden waren und die Wirkung der UV dahingehend konditioniert haben könnten.

Auf staatlicher Ebene begann China Mitte der 1990er Jahre mit dem Aufbau eigener Fähigkeiten im Bereich des Cyberkonfliktaustrages. So wurde 1995 ein ›Information-Warfare-Plan‹ implementiert und ab 1997 wurden Übungen durchgeführt, etwa um ausländische Militärsysteme oder Rundfunkanbieter zu stören. Im selben Jahr wurde zudem eine ca. 100 AkteurInnen umfassende Militäreinheit gegründet, um solche Manipulationsmöglichkeiten vor allem gegen westliche und amerikanische Militärsysteme realisieren zu können (Ball 2011, S. 81). Im weiteren Verlauf wurde ab 2000 die Doktrin der »*Integrated Network Electronic Warfare*« (INEW) auf Ebene der PLA organisatorisch umgesetzt, indem das PLA General Staff Departments (GSD) »*4th Department (4PLA)*« die offensiven Cyber- und Electronic-Warfare-Kapazitäten und das »*3th Department (3PLA)*« die defensiven Cyberfähigkeiten sowie die Befugnisse zur Spionage erhielten (Krekel 2009, S. 6–7). Insbesondere, um diese dezentralisierte Militärstruktur der PLA im Cyberspace stärker zusammenzuführen, wurde 2010 eine »*Cyber-Base*« errichtet, von der westliche BeobachterInnen annahmen, dass sie eine Art chinesisches »*Cyber-Command*« im Rahmen der PLA bedeuten würde. In der chinesischen Global Times zitierte PLA-Offiziere bemühten sich jedoch, klarzustellen, dass diese »*a ›defensive‹ base for information security, not an offensive headquarters for cyber war*« sei (zitiert in: Hsiao 2010). 2015 kam es schließlich zur bereits erwähnten Militärreform innerhalb der PLA, die im Cyberspace vor allem die Einsetzung der SSF sowie de facto eine von nun an stärkere Konzentrierung der PLA auf offensive Cyberoperationen im Rahmen von Konflikten vorsah. Für Cyberspionage im wirtschaftlichen Bereich war von nun an noch stärker das MSS verantwortlich (Kania und Costello 2018, S. 107).

Über die Anfangsphase des staatlichen Cyberkonfliktaustrages ist zudem bekannt, dass es chinesischen AkteurInnen offensichtlich bereits früh gelang, technisch versierte HackerInnen, die sich zuvor zumeist als HacktivistInnen oder patriotische HackerInnen verdingten, in ihre Befehlsstruktur zu integrieren: Im bereits erwähnten US-Geheimdienstbericht von 2009 wurde beschrieben, wie chinesische Geheimdienste mit Firmen zusammenarbeiteten, die wiederum bekannte Hacker rekrutiert hatten. Beispiele hier-

für wurden ebenfalls genannt, etwa der Gründer der Hackergruppe »*The Honkers Union of China*«, Lin Yong, genannt »*LION*« (The New York Times 2009). Für den privatwirtschaftlichen Bereich ist davon auszugehen, dass Unternehmen auf solch eine Kooperation mit staatlichen Behörden zwingend angewiesen waren, wenn das starke Maß an staatlicher Regulierung des chinesischen Wirtschaftssektors bedacht wird. Gleichzeitig wurde unter staatlicher Anleitung im Laufe der Jahre ein wachsender Pool an Technologieunternehmen aufgebaut, nicht zuletzt zur Umsetzung der anvisierten Abschottung des nationalen Intranets durch die ›Great Firewall‹, was ebenfalls im besagten US-Geheimdienstbericht am Beispiel des Unternehmens TOPSEC zum Ausdruck kommt. Hinzu kommt speziell seit Xis Amtsübernahme, dass es chinesischen HackerInnen, etwa MitarbeiterInnen von IT-Unternehmen, ab 2018 untersagt wurde, an ausländischen Hacking-Wettbewerben teilzunehmen. Die KPC strebte mit diesem Schritt offensichtlich an, die technischen Fähigkeiten der eigenen HackerInnen sowie deren entdeckte Sicherheitslücken nicht mehr ins Ausland abfließen zu lassen, sondern zuerst für nationale Zwecke, vermutlich offensive Cyberoperationen, zu nutzen (Gierow 2018).

Auf zivilgesellschaftlicher Ebene wurde insbesondere durch den verstärkten Austausch zwischen chinesischen und westlichen Universitäten am Aufbau des notwendigen technischen Knowhows zur Durchführung von Cyberoperationen gearbeitet. Dies spiegelt sich auch in der Entwicklung der chinesischen Ausgaben im Bereich Forschung und Entwicklung seit 2000 wider (s. Tabelle 14). So stieg die Anzahl chinesischer Studierender in den USA von 1985 bis 2007 stetig an (Laughlin 2008, S. 7). Im Gegensatz zu Russland, das nach dem Zerfall der Sowjetunion zahlreiche, technisch hochgradig qualifizierte WissenschaftlerInnen nicht adäquat in den Arbeitsmarkt integrieren konnte (was auch unter Putins Führung noch ein Problem darstellt(e); Schiermeier 2014, S. 298), war China im selben Zeitraum im wirtschaftlichen Aufstieg begriffen und konnte somit fehlende eigene Kapazitäten im Technologiebereich aufholen und diese gleichzeitig entsprechend des Eigenbedarfes auch effizient in staatliche und quasi-staatliche Strukturen integrieren. Auch auf dem heimischen Wissenschaftsmarkt wurde der Aufbau technischer Fähigkeiten im Cyberspace mithilfe mehrerer Institute und Forschungseinrichtungen forciert. Beispiele sind das dem MSS unterstehende »*Chinese Institute of Contemporary International Relations*«, die »*Chinese Academy of Engineering, Chinese Academy of Science*«, »*Academy of Military Science der PLA*« sowie die »*PLA Information Engineering University*« (Raud 2015, S. 17).

2013 kam es zu einer der ersten Veröffentlichungen eines anonymen Cybercrime-Analysten, der die Identität eines chinesischen Hackers mit Universitätshintergrund entlarvte. Es handelte sich um einen Mitarbeiter der PLA Engineering University (Cyb3rsleuth 2013). Weiterhin interessant ist der Umgang der KPC mit sog. ›Bug-Bountry-Programmen‹: 2018 verbot die Partei chinesischen HackerInnen de facto die Teilnahme an ausländischen Hacker-Wettbewerben (Bing 2018), nachdem 2017 mit dem Tianfu Cup ein nationales Format dieser Art gestartet wurde. BeobachterInnen sahen darin einerseits den Versuch, das Talent nationaler HackerInnen zu nutzen sowie die eigenen Cyberfähigkeiten nach außen zu demonstrieren, andererseits jedoch auch nicht zu viele Informationen über die zur Schau gestellten Hacking-Tools und Exploits preiszugeben (Work 2021).

Der chinesische Cyberkriminalitätsmarkt wurde Anfang der 2000er Jahre noch als moderat bezeichnet. So hatte das hierfür zuständige »*Information Security Supervision Bureau*« des MPS im Jahr 2002 lediglich etwas mehr als 3000 Fälle von Cyberkriminalität berichtet (Broadhurst und Grabosky 2005, S. 8), die jedoch der in diesem Bereich prinzipiell hohen Dunkelziffer sowie behördlichen Anreizen zur Fälschung der Daten geschuldet sein könnten. Die durchaus existierende Gesetzgebung zur Prävention, Verfolgung und Bestrafung von Cyberkriminellen wurde jedoch Mitte der 2000er Jahre als ineffizient bezeichnet, gerade wenn es um die Strafverfolgung solcher AkteurInnen ging (Broadhurst und Grabosky 2005, S. 8). Das Beispiel zweier 1998 zum Tode verurteilter Brüder, die zuvor die Netzwerke einer Bank gehackt hatten, belegt jedoch das im Falle einer Strafverfolgung resolute Vorgehen der KPC gegenüber Cyberkriminellen (Putnam und Elliott 2001, S. 44). Dies gilt besonders für Kriminalität gegen Ziele des nationalen Wirtschafts- und Finanzsektors. Somit könnte die scheinbare Straffreiheit chinesischer Cyberkrimineller nur geduldet sein, solange ihre Aktivitäten den Modernisierungspfad Chinas nicht negativ beeinflussen. Genuine Cyberkriminelle, die etwa im Raum der ehemaligen Sowjetunion vor allem Russland und die Ukraine zu international agierenden Cyber-Crime-Hotspots werden ließen (Kshetri 2013), gab es zu Beginn des Untersuchungszeitraums in vergleichbarem Maße in China nicht. Dies könnte die Auswirkung der noch zu behandelnden UV für China insofern beeinflusst haben, als eher ideologisch motivierte HacktivistInnen sowie als deren Zwischenauftraggeber fungierende domestische Technologieunternehmen als Proxys instruiert wurden. Das beschriebene Moonlighting chinesischer Proxys deutet jedoch auch darauf hin, dass sich diese über die Zeit zumindest in diesem Bereich ermächtigt haben könnten. Dies könnte für die Geheimdienste und letztlich die KPC jedoch insofern tolerierbar sein, als diese mit ihren zumindest im Rahmen dieser Analyse beschriebenen Tätigkeiten ausländische Zielsysteme anvisierten und nicht mehr, wie noch zu Beginn des Untersuchungszeitraumes, inländische. Die von Proxy-Operationen ausgehenden Eskalationsrisiken werden für die Analyse der UV in Beziehung zur jeweiligen allgemeinen Konfliktintensität mit dem staatlichen Gegenüber gesetzt.

Zusammenfassend wird konstatiert, dass die Ausprägungen der KV für China direktstaatliche Cyberoperationen, vor allem aber im privatwirtschaftlichen sowie zivilen Bereich Proxy-Operationen prinzipiell zuließen und somit das Wirken der UV mutmaßlich dahingehend konditioniert haben. China fokussierte den Aufbau an technischem Knowhow bereits vor Beginn des Untersuchungszeitraumes und schuf somit die notwendigen Bedingungen für die beschriebene Proxy-Nutzung.

Tabelle 14 listet die jeweiligen Ausprägungen der NCPI-Teilindikatoren auf.

Tabelle 14: Chinas Cyber-Akteursumwelt auf staatlicher/privatwirtschaftlicher Ebene

NCPI-Teilindikatoren *(staatliche Ziele)*	Ausprägung/Schwerpunkt
Cyber (related) Military Doctrines *(Offense)*	Doktrin der »*Integrated Network Electronic Warfare*« ab 2000 Zweijährliches Defense-White-Paper (DWP, ab 2004), erstmalige Erwähnung des Begriffes ›Cyber‹ im Jahr 2010 (Hsu et al. 2013, S. 9) DWP 2015: Cyber- und Space-Domänen als »*commanding heights of strategic competition*« (Fravel 2015, S. 4)
National Cyber Command/Cyber (Military) Staffing *(Offense)*	*Militär:* Militäreinheit zur Umsetzung des »*information warfare plan*« aus 1995 (Ball 2011, S. 81) »*Information Security Base*« (xinxi baozhang jidi), aka »*Cyber Command*« seit 2010 (Hsiao 2010) PLA »*Cyberspace Strategic Intelligence Research Center*«, gegründet 2014 (Gertz 2014a) Dominantes Department bis 2015: 3PLA (Gertz 2016a) SSF der PLA ab 2015 (Kania und Costello 2018) *Zivile Geheimdienste:* *Ministry of State Security*, verantwortlich für Auslands- und Gegenspionage, jedoch auch Überwachung im Inland. *Ministry of Public Security*, verantwortlich für die Verfolgung von Cyberkriminellen, den Schutz kritischer Infrastrukturen und die Great Firewall of China. Ist jedoch auch in domestische Spionage involviert (Raud 2015, S. 17).
Global Top Technology, Cybersecurity Firms *(Offense, Commercial Gain, Intelligence)*	*International agierende IT-Unternehmen (u.a.)* Huawei Tencent ZTE Alibaba (z.B. Alipay als Online-Zahlungsmittel) *Domestisch konzentrierte IT-Unternehmen (u.a.)** Boyusec Chengdu Shirun Technology Company Ltd. Chengdu Hanke Technology Company Ltd. Chengdu Xinglan Technology Company Ltd. Hainan Xiandun Technology Company Antorsoft Jinan Quanxin Fangyuan Technology Co. Ltd. Jinan Anchuang Information Technology Co. Ltd. Jinan Fanglang Information Technology Co. Ltd. RealSOI Computer Network Technology Co. Ltd. Huaying Haitai Science and Technology Development Co Ltd. Laoying Baichen Instruments Equipment Co Ltd.

High-Tech Exports *(Offense, Commercial Gain, Intelligence)*	Von 2007 bis 2019 mit ca. 30 Prozent an den Gesamtindustrieexporten des Landes auf einem stetig konstanten Niveau, dabei weit über dem Niveau Russlands (ca. zwischen 7 und max. 16 Prozent im selben Zeitraum), ab 2013 jedoch z.B. unterhalb der Rate von Vietnam (World Bank 2020).[49] Chinas Forschungs- und Entwicklungsausgaben lagen dabei jedoch deutlich über dem der beiden anderen Autokratien, mit ca. 0,9 Prozent (2000) und 2,2 Prozent (2018) am Gesamt-BIP (World Bank 2021c).

(Eigene Darstellung)
*Quelle: Intrusion Truth Blogposts. Weitere chinesische IT-Unternehmen finden sich in Morgan 2020 u.a. auch Qihoo 360, das eigene Attributionsberichte in ›westlicher Manier‹ veröffentlicht.

5.3.3 Chinas domestische Präferenzkonstellationen und der Einfluss des allgemeinen Konfliktniveaus

Wirtschaftsspionage gegenüber den USA, Europa sowie asiatischen Ländern kann als das zentrale Charakteristikum chinesischer Cyberoperationen im Allgemeinen sowie chinesischer Proxyoperationen im Konkreten bezeichnet werden. Neben politischer Spionage im Cyberspace, die wie der OPM-Hack zwar große Aufmerksamkeit und politische Resonanz erfuhr, rechtlich gesehen jedoch nach wie vor weitgehend ›Fair Game‹ zwischen Staaten zu sein scheint, entfachte dieser strategische Diebstahl geistigen Eigentums den größten Widerstand der betroffenen AkteurInnen. Diese externen Faktoren führten neben internen Faktoren zur aufgezeigten Umstrukturierung der offensiven Cyberkonfliktstruktur chinesischer Behörden und deren Proxys. Dabei wurden die bei der Analyse der KV identifizierten technischen Voraussetzungen gerade im kommerziellen Bereich intensiviert und für das Auslagern von Cyberoperationen an Proxys genutzt. Es wird analysiert, inwiefern welche Präferenzkonstellationen auf den drei Ebenen des Liberalismus zu welchen Änderungen im aufgezeigten inhaltlichen sowie organisatorischen Cyberkonfliktaustrag Chinas geführt haben. Neben der scheinbaren Konstante der Wirtschaftsspionage gilt es auch zu beleuchten, inwiefern der Einfluss der IV, gerade im Rahmen des Konfliktes um das Südchinesische Meer, zur aufgezeigten Erweiterung des funktionalen Proxyportfolios beigetragen hat und welche Formen von Cyberoperationen hieraus resultierten. Besagte Wirkweise der IV wird somit in die Betrachtung der UV integriert, um eine möglichst leserfreundliche und weniger redundante Darstellungsweise gewährleisten zu können.

Bevor jedoch die Präferenzkonstellationen Chinas auf domestischer Ebene als Haupterklärungsfaktor für dessen Cyberproxy-Strategie herangezogen werden können, muss eine Identifikation der hierbei maßgeblichen Regimeeliten erfolgen. Nur wenn (auch im Zeitverlauf) aufgezeigt werden kann, welche Teile der Winning Coalition durch formelle oder informelle Prozesse und Regularien auf republikanischer

49 »*High-technology exports are products with high R&D intensity, such as in aerospace, computers, pharmaceuticals, scientific instruments, and electrical machinery*« (World Bank 2020).

Ebene die Präferenzen des Landes auf ökonomischer sowie ideeller Ebene maßgeblich beeinflussten, können diese wiederum analysiert werden.

5.3.3.1 Das Who's Who der chinesischen Winning Coalition

Die Politik der VR China wird seit ihrer Gründung 1949 maßgeblich durch die Kommunistische Partei dominiert. Entsprechend der Regimetypenklassifizierung nach Kailitz wäre das Land aus ideologischer Sicht aufgrund seiner historischen Entwicklungsgeschichte als kommunistische Ideokratie zu bezeichnen. Werden dagegen stärker institutionalistische Kriterien angelegt, müsste China aufgrund des weisungsbefugten Charakters der KPC als Staatspartei eher als Einparteienregime klassifiziert werden (Heilmann 2018). Diese Sicht teilten aufgrund der dominanten Rolle der KPC in nahezu allen Lebensbereichen des Landes bislang die meisten BeobachterInnen (vgl. Stathis N. Kalyvas 1999; O'Brien und Li 2000; Snape und Wang 2020). Bereits seit der Gründung der VR im Jahr 1949 unter Mao Zedong besitzt die Partei mit heute über 90 Millionen Mitgliedern de facto das Machtmonopol im Land. Als Basis dienen hierbei die drei Machtsäulen der »*Control of Personel, Propaganda, and the People's Liberation Army*« (Albert et al. 2021). Auf institutioneller Ebene übt die KPC ihre Macht über die zentrale Militärkommission der PLA aus, der Xi Jinping seit 2012 vorsteht. Auch wenn die KPC nach außen hin oftmals das Image einer homogenen, vereinten Partei vermittelt, steht ›Factional Infighting (*neidou*)‹ bereits seit den Tagen Mao Zedongs an der Tagesordnung, mit pragmatischer und wenig loyalitätsbasierter Allianzbildung (Tse 2018).

Die Anziehungskraft sowie Funktionsweise der KPC wurden in den 1990er Jahren aufgrund der durch den wirtschaftlichen Aufstieg grassierenden Korruption nicht positiv bewertet: »[…] *economic reforms facilitated the illicit conversion of political power into economic gains, causing a breakdown of the state's institutional discipline and fueling an exodus from the party*« (Stathis N. Kalyvas 1999, S. 340). Wohl auch deshalb nahm die Anzahl der KPC-Mitglieder von 2002 bis 2012 und somit bis zur Amtsübernahme Xi Jinpings stetig zu (Thomas 2020). Als Gründe hierfür wurden vor allem die mit der Parteimitgliedschaft verbundenen sozio-ökonomischen Vorteile genannt. Diese hatten den Willen zur Verwirklichung der kommunistischen Ideologie im Laufe der Jahre als Hauptbeweggrund immer stärker abgelöst, nicht zuletzt aufgrund des von der KPC forcierten Entwicklungs- und Modernisierungspfades des Landes (The Straits Times 2017).

Gleichwohl dürfte die KPC diese zahlenmäßige Erweiterung ihrer Machtbasis auch für deren qualitative Stärkung genutzt haben: Somit konnten Parteimitglieder direkt, über deren Kontrollfunktionen indirekt auch Nichtmitglieder, effektiver überwacht werden. Speziell bei einem flächenmäßig so großen Land mit vielen regionalen Ablegern staatlicher und politischer Behörden erschien dieser Personalaufwuchs dringend notwendig. Diesen Ansatz brach Xi Jinping jedoch insofern, als er weniger OpportunistInnen und stärker LoyalistInnen in den Parteireihen bevorzugte, um die gesamtstaatlich ›richtigen‹ Anreize zu einem Parteibeitritt zu setzen (Thomas 2020). Entsprechend seiner nachdrücklich verfolgten Antikorruptionskampagne bemühte er sich daher in der Folge, den Grundsatz ›Qualität vor Quantität‹ auch bei der Parteimitglieder-Rekrutie-

rung als oberste Prämisse zu etablieren (Jinping 2018).[50] Er betonte diesen Grundsatz bereits 2013 in einem Treffen des Politbüros (Xinhua 2013), das zusammen mit dem ständigen Ausschuss das Zentralkomitee bildet und wie die Militärkommission auch Xi Jinping als Generalsekretär der KPC unterstellt ist. Die Position des Generalsekretärs der KPC kann als parteipolitisches Äquivalent zu Xis Staatspräsidentenamt auf staatlicher Ebene bezeichnet werden. Der KPC kommt jedoch durch ihre Befugnisse zu Leitlinien, Weisungen, politischer Kontrolle sowie der angesprochenen Kaderpolitik die zentrale Machtposition in Chinas politischem System zu, ohne dass es institutionelle VetospielerInnen oder Kontrollmechanismen gäbe (Heilmann 2018). In der derzeit noch gültigen Version der Verfassung von 1982 wurden daher die Stabilisierung der Institutionen des Staates, also vor allem der KPC selbst, sowie die ›sozialistische Modernisierung‹ des Landes im Sinne der »*Four Modernizations*«, »*industry, agriculture, defense, and science and technology*« als Hauptziele Chinas ausgegeben (Jones 1985, 713, 726). Auch wenn es keine Beschränkung der Machtposition der KPC durch Dritte gibt, führte der damalige de facto Staatsführer Deng Xiaoping infolge des Todes Mao Zedongs innerhalb der Partei institutionalisierte Regelungen ein, um den Aufstieg eines weiteren Diktators in Zukunft zu verhindern (Shirk 2018, S. 22). Diese umfassten etwa die Beschränkung und Limitierung der Amtszeiten des Präsidenten, die Implementierung des Staatsrates und somit des Kabinetts der VR China sowie die Stärkung weiterer KPC-Institutionen wie des Zentralkomitees und des Ständigen Ausschusses des Politbüros. Durch diese Dezentralisierung der Macht sollte gewährleistet werden, dass die KPC als Ganzes und nicht etwa ein zu stark ermächtigter Einzelner das Gravitationszentrum der Macht darstellte (Shirk 2018, S. 22).

Speziell unter der Führung Xis bemerkten verschiedene BeobachterInnen jedoch eine verstärkte Personalisierung sowie Rezentralisierung der Machtstrukturen innerhalb der KPC (Mao 2021, 7). So ging er von Anfang an hart gegen parteiinterne GegnerInnen, etwa den linkssozialistischen Bo Xilai, vor. Dieser stellte eine ernsthafte Gefahr für die marktliberalistischen Präferenzen Xis dar und wurde letztlich u.a. wegen Korruption und Machtmissbrauch zu einer lebenslangen Gefängnisstrafe verurteilt (Richter 2013). Während unter Hu Jintao KPC-Mitglieder ihre eigenen Patronage-Netzwerke noch freier aufbauen und pflegen konnten, wurde ihnen dies unter Xis Führung zunehmend erschwert (Shirk 2018, S. 24). Zudem gelang es Xi immer effektiver, die von seinen Vorgängern etablierten internen Checks and Balances außer Kraft zu setzen. Ein konkretes Beispiel hierfür ist die Aufhebung der Amtszeitenbeschränkung 2018, die den über 2023 hinausgehenden Machtanspruch Xis andeutete (Doubek 2018). Hierbei handelt es sich um eine klare Abkehr von der friedlichen »*leadership succession*« (Meng 2021), einem Hauptbestandteil der bemerkenswerten Resilienz des Einparteienregimes auf institutionalistischer Ebene. Von diesem Prinzip hatte Xi zuvor noch selbst profitiert, da er ab 2008 Vizepräsident war und de facto bereits als Nachfolger von Hu inthronisiert wurde

50 Hinsichtlich der Rekrutierungsstrategie im Falle der PLA fand eine aktuelle Studie aus dem Jahr 2021 heraus, dass die KPC offensichtlich in Zeiten verstärkter domestischer Bedrohungen vermehrt auf loyale, jedoch oftmals weniger kompetente PLA-OffizierInnen setzte. Im Gegenzug wurde in Zeiten intensivierter externer Bedrohungslagen wiederum verstärkt auf Kompetenz und weniger Loyalität bei der Auswahl der Militärmitglieder gesetzt (Mattingly 2021).

(Cabestan 2009, S. 71). Auch gegenüber dem bewaffneten Arm der KPC, der PLA, verfolgte Xi seit Beginn seiner Amtszeit einen strategischen, auf die eigene Machtausweitung ausgerichteten Ansatz: So setzte er beim 18. Parteikongress 2012 noch auf ihm getreue PLA-OffizierInnen. Fünf Jahre später, als er seine persönliche Machtbasis mittlerweile auch mit deren Hilfe hinreichend ausgebaut hatte, berief er diese jedoch nicht mehr als Mitglieder des 19. Parteikongresses (Mattingly 2021, S. 29). Der für den Untersuchungszeitraum ebenfalls relevante frühere KPC-Generalsekretär und Staatspräsident Hu Jintao (2002–2012) wurde jedoch im Gegensatz zu Xi als weitaus schwächer mit der PLA vernetzt angesehen. Somit wurden auch dessen faktische Kontrolloptionen gegenüber dem Militär als schwächer beurteilt. Im Gegensatz dazu wurde Xis Modus Operandi der Machtkontrolle gegenüber dem Militär folgendermaßen beschrieben:

> »No other Chinese Communist Party leader, not even Mao Zedong, has controlled the military to the same extent as Xi does today. Mao had to share power with powerful revolutionary-era marshals.« (Cheung 2017, S. 12)

Dieses Streben nach absoluter Macht betraf auch die veränderte Befehlsgewalt gegenüber der ›People's Armed Police‹, einer paramilitärischen Polizeieinheit, die vor Xis Amtszeit sowohl der Militärkommission als auch dem Staatsrat unterstellt war, seit seiner Amtsübernahme jedoch nur noch Ersterer mit Xi als Vorsitzendem unterstellt ist (Shirk 2018, S. 24).

Als zentrale AkteurInnen der chinesischen Winning Coalition werden für die Analyse der UV somit vor allem die KPC, stets in Bezug zu ihrem jeweiligen Anführer, Hu Jintao vs. Xi Jinping, sowie die PLA identifiziert. Diesen AkteurInnen wird der größte Einfluss auf die Außen- und Sicherheitspolitik des Landes und dessen Cyberproxynutzung zugesprochen. Xi Jinping wird aufgrund seiner personalistischen Herrschaftsführung eine besondere Bedeutung beigemessen. Gleiches gilt für dessen Präferenzen für den chinesischen Cyberproxy-Austrag ab 2012. Die Interessen der PLA werden in Abhängigkeit zur KPC unter dem jeweiligen Generalsekretär betrachtet, entsprechend der verbreiteten Einschätzung, dass sie eine Parteienarmee ist (Paul 2018, S. 20). Alle hochrangigen PLA-OffizierInnen sind zugleich KPC-Mitglieder, andersherum sind auch in zentralen Parteiinstitutionen oftmals PLA-Mitglieder vertreten. Entsprechend der prominenten Rolle des MSS bei der chinesischen Proxy-Anleitung wird es ebenfalls in Abhängigkeit zur KPC in die Analyse inkludiert. Auch wenn es auf institutioneller Ebene dem Staatsrat und somit Xi Jinping nicht direkt unterstellt ist, weitete Xi Jinping auch über diese Institution seine Macht weiter aus, insbesondere seit der Forcierung der Anti-Korruptionskampagne sowie Umstrukturierung des Militär- und Sicherheitsapparates ab 2015. So ernannte er mit Chen Wenqing 2015 einen früheren stellvertretenden Sekretär der von Xi eingesetzten ›Central Commission for Discipline Inspection‹ (CCDI) zum Leiter des MSS (Mattis 2015b).[51]

---

51 Auch wenn dem MPS oftmals eine ebenfalls dominante Rolle in China's Cyberpolitik attestiert wird, ist diese entsprechend seines Mandats doch eher domestisch orientiert. Die Überwachungsmaßnahmen werden weniger durch Hackingoperationen, als durch die Kontrolle der nationalen IT-Infrastruktur (›Great Firewall of China‹) ermöglicht und daher nicht in die Analyse aufgenommen (vgl. Jones 2020; Frankenberg 2020).

Zuletzt wird in geringerem Umfang analysiert, inwiefern es im Untersuchungszeitraum zur Ausbildung einer eigenständigen Wirtschaftselite im Informationstechnologiesektor kam. Können Unternehmen wie Alibaba, Tencent und Huawei sowie deren teilweise prominenten Chefs wie Jack Ma als Vetospieler zur KPC betrachtet werden und welche Rolle kann ihnen bei der Präferenzartikulierung und -verfolgung durch Cyberoperationen zugesprochen werden?

5.3.3.2 Die KPC im Wandel der Zeit – zwischen ökonomischer Liberalisierung und politischem Nationalismus

Den Interessen der KPC wird aufgrund des Charakters der VR China als Einparteienregime die größte Relevanz im Hinblick auf die Erklärung der chinesischen Cyberoperationen zugesprochen. Nachfolgend werden diejenigen Interessen herausgegriffen, die die chinesische Präferenzordnung unter den beiden Führern Hu Jintao und Xi Jinping am stärksten mitbestimmten. Dabei wird untersucht, inwiefern diese Präferenzkonstellation die chinesischen Cyberproxyoperationen erklären kann und welche Interdependenzen gegenüber welchen AkteurInnen berücksichtigt bzw. adressiert wurden.[52]

Die KPC unter Hu Jintao

Für den gesamten Zeitraum der Ägide unter Hu Jintao (2002–2012) kann die Erstarkung einer parteiideologischen Legitimationsbasis der KPC festgestellt werden. Konfrontiert mit den Defiziten einer ausschließlich performanzbasierten Legitimationsstrategie, wie sie unter Deng Xiaoping forciert wurde, bemühte sich die KPC, durch eine Wiederbelebung kommunistisch-marxistischer Elemente hierauf zu reagieren (Holbig 2009).[53] Ein verstärkter Fokus auf Parteiideologie sollte somit dem ›Performance-Dilemma‹ der KPC entgegenwirken, nach dem der zahlenmäßig rasante wirtschaftliche Aufstieg des Landes in sozialer Ungleichheit und Unzufriedenheit mündete, was zusätzliche Legitimationsquellen erforderlich machte (Holbig und Gilley 2010, S. 400). In Zeiten wirtschaftlichen und sozialen Wandels sollten ideologische Elemente als Garant der gesellschaftlichen Einheit und letztlich parteipolitischen Stabilität dienen. Als Hauptanker dieser parteiideologischen Grundausrichtung der KPC fungierten die 2000 noch unter Jiang Zemin formulierten »*Three Represents*«. Diese repräsentieren die »*development trends of advanced productive forces.* […] *the orientations of an advanced culture.* […] *the fundamental interests of the overwhelming majority of the people of China*« (China.org 2003). Die wirtschaftliche Entwicklung war auch noch während Hu Jintaos Präsidentschaft das Hauptinteresse der KPC. Wie die vorherigen Ausführungen jedoch zeigen, galt es, dieses infolge tiefgreifender Transformationsprozesse auf ökonomischer sowie sozialer Ebene verstärkt mit anderen Interessen, allen voran der gesellschaftlichen Kohäsion zur Stabilisierung der Parteienherrschaft, in Einklang zu bringen. Nachfolgend wird somit aufgezeigt, auf

52 Wenn nachfolgend auf Zahlen aus dem HD-CY.CON verwiesen wird, beziehen sich diese auf dieselben 115 Operationen wie unter 5.3.1.1.

53 »*The prioritization of economic growth has resulted in political incentive structures for cadres which have bred corruption and abuse of power, local »palace economies«, and a common disregard for social matters*« (Holbig 2009, S. 42).

welche Weise dieses Dilemma die Politik unter Hu Jintao auf domestischer und außenpolitischer Ebene prägte. Durch diese Analyse der in diesem Zeitraum prävalenten Interessenlage der KPC soll in einem weiteren Schritt der inhaltliche Fokus chinesischer Cyberproxyoperationen im Zeitraum von 2003 bis 2012 erklärt werden (n = 42 von 115).

›*Harmonious Society*‹: Gesellschaftliche Einheit trotz wirtschaftlicher Entwicklung

Hu Jintao sah sich zu Beginn seiner Amtszeit mit dem Umstand konfrontiert, dass sich die VR China zwar in den 1990er Jahren zu einer Art ›Economic Miracle‹, gleichzeitig jedoch auch zur ›Werkbank der Welt‹ entwickelt hatte (Harrison und Palumbo 2019). Konkret bedeutete dies einerseits einen rasanten Anstieg des BIP des Landes, andererseits jedoch auch der gesellschaftlichen Ungleichheit im Land. So ging die Spannweite zwischen arm und reich, zwischen dem Land und den Städten bis 2008 immer weiter auseinander (Jain-Chandra et al. 2018). Den zeitweiligen Höhepunkt der ökonomischen Entwicklung markierte der WTO-Beitritt der VR im Jahr 2001. Nach langen Verhandlungen mit den USA und der EU kam es schließlich zu dieser laut damaligem Staatschef Jiang Zemin ›Win-win‹-Option. Innerhalb der Partei hatten sich die Globalisierungsbefürworter gegen kommunistisch orientierte VertreterInnen des linken Spektrums durchgesetzt. Im Lager der westlichen Staaten beflügelte der WTO-Beitritt der VR dagegen liberal geprägte Hoffnungen, China werde hierdurch einerseits vollständig in das globalisierte Interdependenzgeflecht eingebunden und andererseits im Inneren demokratisiert (Kahl 2001, S. 424–425).

Die beschriebene soziale Ungleichheit führte während der Amtszeit von Hu Jintao ferner zu verstärkten domestischen Unruhen, auf die das Regime mit einer »*Strike Hard, Maximum Pressure*«-Kampagne reagierte (Merkley und McGovern 2006).[54] In einer für autokratische Regime oftmals typischen Weise wurden dabei Aufständische und Protestierende mit TerroristInnen und Kriminellen gleichgesetzt und somit gewaltsame, repressive Gegenmaßnahmen gegen diese legitimiert. Besonders ging es dabei um die Eindämmung der aus KPC-Sicht separatistischen Gefahr aus der Region Xinjiang, die hauptsächlich von der muslimischen Minderheit der Uiguren bewohnt ist. Dabei wurde das Narrativ des »*War on Terror*« in Folge von 9/11 genutzt, um die sog. »*Three Evil Forces*« – Terrorismus, Separatismus und religiöser Extremismus – zu bekämpfen (Human Rights Watch 2007, S. 265). Das Interesse der KPC, diese Akteursgruppierungen zu kontrollieren und in Schach zu halten, um die soziokulturelle Einheit des Landes mit den Han-ChinesInnen als dominierender Gruppierung zu gewährleisten, spiegelt sich im HD-CY.CON jedoch erst für die Zeit der Präsidentschaft Xi Jinpings stärker wider. So wurde bis 2012 lediglich eine Cyberspionageoperation gegen die autonomen Gebiete Tibet und Xinjiang verzeichnet (ab 2009 durch Winnti). Zudem wurde im Falle der Operation Aurora (2009–2010) von ausspionierten chinesischen MenschenrechtsaktivistInnen seitens APT17 berichtet. Insgesamt verließ sich das Regime in dieser früheren Phase des Cyberkonfliktaustrages öffentlichen Berichten zufolge gegenüber Tibet und Xinjiang jedoch noch stärker auf Zensur und die zeitweilige Abschaltung des Internets in der Region, nachdem es dort im Juli 2009 zu gewaltsamen Ausschreitungen gekommen war

54 So hat sich die Anzahl an sozialen Unruhen von 1993 bis 2005 verzehnfacht (Göbel und Ong 2012, S. 8).

(Branigan 2009). Ein Grund hierfür könnte sein, dass speziell das Anliegen der Uiguren erst unter Xi Jinping verstärkt in den Fokus der westlichen Aufmerksamkeit geraten ist und sich in dieser Zeit auch westliche JournalistInnen und AktivistInnen verstärkt mit deren Schicksal befasst haben (Deutsche Welle 2008a; Der Tagesspiegel 2021). Schwerer zu enttarnende Cyberoperationen könnten somit erst unter Xi Mittel der Wahl gegenüber den Uiguren geworden sein, um die zunehmend konfliktive Präferenzkonstellation zu westlichen Demokratien auf ideeller Ebene zu manipulieren.

Um auf die beschriebenen gesellschaftlichen Ungleichheiten zu reagieren, entwickelte Hu Jintao im Einklang mit dem verstärkten Fokus auf parteiideologischen Elementen das Prinzip der »*Harmonious Society*« (*hexie shehui*) (Zheng und Tok 2007). Dabei stand die Anpassung der wirtschaftlichen Erfolgsgeschichte der VR im Hinblick auf eine nachhaltigere Entwicklung im Vordergrund. Dies entsprach einem der Hauptinteressen der KPC in dieser Zeit, stärker die soziale Einheit der Bevölkerung in den Blick zu nehmen (Zheng und Tok 2007, S. 8). Als Vorgänger-Prinzip von ›Harmonious Society‹ diente daher »*Scientific Development*« (*kexue fazhanguan*), dessen Schwerpunkt sich auch im technokratischen Hintergrund der Mitglieder des Ständigen Komitees des Politbüros zwischen 2002 und 2012 widerspiegelte (Brown und Bērziņa-Čerenkova 2018, S. 326).[55] China wollte sich nach und nach von der zuvor dominierenden industriellen Massenherstellung lösen. Der elfte Fünfjahresplan der VR markierte mit der darin formulierten Zielsetzung, die VR zu einem ›innovativen Staat‹ aufzubauen (China.org 2006), den Startschuss für diesen Strategiewandel. Als konkrete Zielsektoren wurden darin nachhaltigere Energietechnologien benannt, um den eigenen Ressourcenbedarf effizienter decken zu können und die Umwelt weniger zu belasten. Das Interesse der KPC unter Hu Jintao an einer nicht nur zahlenmäßigen Wirtschaftsentwicklung, sondern dem Identifizieren einzelner Technologiesektoren, in denen China mittelfristig eine Führungsposition anstrebte, kann das dominante Profil chinesischer Cyberoperationen von 2003 bis 2012 plausibel erklären. Gleichzeitig verdeutlicht es, dass sich die Präferenzordnung der KPC im Laufe der Jahre notwendigerweise gewandelt hat. So wurde Wachstum nicht mehr um jeden Preis forciert, sondern sollte künftig stärker mit anderen Interessen der Partei, speziell einer vereinten und ›zufriedenen‹ Bevölkerung, in Einklang gebracht werden. Gemäß der Bedeutung wirtschaftlicher Output-Legitimation für die KPC galt es somit, das Interesse an wirtschaftlicher Entwicklung mit den Interessen der Bevölkerung an einem zumindest besseren Lebensstandard stärker in Einklang zu bringen. Der damalige Minister für Wissenschaft und Technik, Xu Guanhua, betonte bei der Präsentation des elften Fünfjahresplans 2005 hierfür die Notwendigkeit der eigenen Innovationsstärkung, um hohe Patentrechtszahlungen an ausländische KonkurrentInnen in Zukunft vermeiden zu können (China.org 2006). Ungesagt blieb an dieser Stelle, dass die VR bereits zu diesem Zeitpunkt auf eine lange Historie an Wirtschaftsspionage zurückblicken konnte, um eben jenes Patentrecht illegaler Weise umgehen zu können. Dabei standen traditionell in erster Linie die USA im Zentrum chinesischer Aktivitäten (Holt 2020). Um diese Interdependenzasymmetrien auf wirtschaftlicher Ebene somit zum eigenen Vorteil zu

55 Das Prinzip des »*Scientific Developments*« rekurrierte dabei auch auf Prinzip des Philosophen Mengzi, »*putting people first‹/'person as the core*« (yi ren wei ben), um der steigenden Kritik an der offenkundigen Korruption der KPC vorzubeugen (Brown und Bērziņa-Čerenkova 2018, S. 327).

gestalten, verlagerte die VR China ihre Spionageaktivitäten immer stärker auf den Cyberspace und nutzte so gleichsam den US-Angriffsvektor, bestehend aus den zahlreichen vernetzten, jedoch oftmals nur schlecht geschützten Unternehmen, zunehmend aus.[56] Im HD-CY.CON drückt sich dies bis 2012 durch 24 verzeichnete chinesische Cyberproxyoperationen aus, in denen Unternehmen und/oder BetreiberInnen des Energiesektors, einem der bedeutendsten Innovationssektoren des Landes, von Spionage betroffen waren. Hauptziele waren dabei US-Entitäten entsprechend deren technologischer Vormachtstellung in den meisten Wirtschaftssektoren. Der Diebstahl geistigen Eigentums half in der Vergangenheit diversen chinesischen Unternehmen, ihre Abhängigkeiten z.B. von US-Unternehmen zu reduzieren und letztere gleichzeitig stärker verwundbar zu hinterlassen (Zarroli 2018). Hierbei handelte es sich um eine gezielte Manipulation der bestehenden Interdependenzasymmetrien mithilfe von Cyberspionage, um das Interesse der ›nachhaltigeren Wirtschaftsentwicklung‹ vorantreiben zu können. Somit wurde letztlich das Erreichen besagter ›Harmonious Society‹ angestrebt, um die wirtschaftlichen Ziele zu erreichen, gleichzeitig jedoch die wachsenden sozialen Unruhen nicht zu einer tatsächlichen Gefahr für die Partei und das ideelle Interesse einer kohäsiven Gesellschaft werden zu lassen. Theoretisch gesprochen manipulierten die chinesischen Cyberproxyoperationen das wirtschaftliche Interdependenzverhältnis besonders zu den USA, um u.a. nach innen die wirtschaftliche Entwicklung stärker im Einklang mit den grundlegendsten Bedürfnissen der eigenen Bevölkerung zu halten.

***»Building an harmonious world« und »Going out«:* Wirtschaftliche Modernisierung und internationale Selbstermächtigung**

Das ideologische Pendant auf außenpolitischer Ebene zur ›Harmonious Society‹ stellte das Prinzip der ›Harmonious World‹ dar. Nach dem Ende der Mao-Diktatur hatte dessen Nachfolger Deng Xiaoping die chinesischen Ambitionen auf außenpolitischer Ebene zurückhaltend formuliert, entsprechend der Grundsätze *taoguang yanghui* (滔光养晦, *to bide one's time*) und *budangtou* (不当头, *not to claim leadership*):

> »In view of all the doubts and uncertainties about the possible outcome of this unprecedented attempt at modernization, and given China's dependence on the international community's constructive support, Deng decided to opt for a course of restraint in foreign policy, particularly since the international community had started to observe the reform process with increasing skepticism after the Tiananmen massacre of June 4, 1989.« (Gareis 2013)

Die damals existierenden Abhängigkeiten sprachen somit für eine passive, auf Kooperation ausgerichtete Außenpolitik der VR, um potenzielle GeldgeberInnen und InvestorInnenländer durch zu aggressives Verhalten nicht zu verschrecken, speziell in Folge der

56 Als konventionelles Pendant zu dieser Praxis können die speziell zwischen 2006 und 2008 stark angestiegenen Foreign Direct Investments (FDIs) chinesischer Unternehmen gelten (CEIC 2021). Diese wurden zu mehr Engagement im Ausland ermutigt, um der KPC dort auch auf analoger Ebene einen direkteren Einflusshebel bieten zu können. Zudem startete China unter Hu Jintao die im Rahmen der OBOR-Initiative perfektionierte Praxis der Entwicklungshilfe und des Leihens von Krediten an Dritte Welt-Länder (Kjøllesdal und Welle-Strand 2010).

negativen Berichterstattung über das Tiananmen-Massaker 1989. Dabei wurde der bereits 1954 begründete pragmatische Grundsatz der »*Five Principles for Peaceful Coexistence* (heping gongchu wu xiang yuanze 和平共处五项原则)« weitgehend fortgeführt (Zhou 2015, S. 212). Wirtschaftliche Entwicklung rangierte somit innerhalb der Präferenzordnung der KPC ganz oben, noch vor potenziellen außenpolitischen Zielen. Unter Jiang Zemin wurde Chinas Außenpolitik dagegen proaktiver, da auf wirtschaftlicher Ebene zu diesem Zeitpunkt bereits erhebliche Erfolge erzielt worden waren. Im Sinne der Prinzipien »*gearing with the world*« sowie »*developing China into a comprehensive power*« agierte die VR fortan selbstbewusster gegenüber der internationalen Staatengemeinschaft, neoliberales Gedankengut verbreitete sich und das Land nahm in IOs eine zunehmend aktive Rolle ein (Zheng und Tok 2007, S. 4).[57] Neben dem konstanten Interesse an der wirtschaftlichen Entwicklung rückte für die KPC unter Jiang Zemin somit die proaktivere Verfolgung chinesischer Interessen auf außenpolitischer Ebene in den Fokus. Konkret bedeutete dies insbesondere ein härteres Vorgehen gegenüber Taiwan, einer der ›Five Poisons‹. Hu Jintao gelang es jedoch nach seiner Amtsübernahme, sich von der konfrontativen Politik seines Vorgängers durch eine pragmatischere Taiwan-Politik abzugrenzen. So pflegte er Kontakte auf taiwanesischer Seite, um die dortige Unabhängigkeitsbewegung in Schach zu halten, und gewährte dem taiwanesischen Volk ökonomische Privilegien (Chang und Chao 2009, S. 112). Während Hus Amtszeit wurden vier chinesische Cyberoperationen gegenüber (u.a.) taiwanesischen Zielen verzeichnet, was mit der beschriebenen Forcierung verstärkter bilateraler Beziehungen zwischen den Ländern unter seiner Führung zusammenfällt. Im Gegensatz zu Tibet und Xinjiang versprachen Cyberoperationen jenseits domestischer Internetkontrolle bereits zum damaligen Zeitpunkt einen größeren Nutzen. Dabei stand das Ausspionieren politischer AkteurInnen und Institutionen im Vordergrund, was durch das beschriebene Interesse der KPC an intensivierten Beziehungen zur taiwanesischen Regierung zum damaligen Zeitpunkt zu erklären ist. Durch politische Cyberspionage kann sich ein Land im Falle von Verhandlungen einen wichtigen Wissensvorsprung verschaffen. Somit dienen Cyberoperationen der Schaffung von Informationsasymmetrien, um die Verwundbarkeit des Gegners bei Verhandlungen zu vergrößern.

Auch gegenüber Ländern wie den USA, Großbritannien, Deutschland, Japan, Kanada, Südkorea und Vietnam wurden diverse Cyberspionageoperationen unter der Ägide von Hu im Datensatz verzeichnet. Die dabei oftmals politischen sowie militärischen Ziele belegen das langjährige Interesse der KPC, nicht nur geistiges Eigentum für innenpolitische Zwecke zu stehlen, sondern sich auch im Rahmen der forcierten Neuorientierung auf außenpolitischer Ebene einen Vorteil zu verschaffen. Nachdem die VR 2001 den Beitritt zur WTO erreicht hatte, positionierte sie sich auch in anderen Organisationen wie der UN unter Hu prominenter. So nahm die Beteiligung Chinas an (Hefele et al. 2015, S. 63) UN Friedensmissionen seit 2004 beständig zu (Gowan 2020). Zeitgleich forcierte Peking den Aufbau regionaler Institutionen, z.B. der SOZ, ebenfalls im Jahr 2001. Auch auf kultureller Ebene wurden chinesische Interessen im Ausland zunehmend

---

57 »*Mao Zedong enabled Chinese to stand tall; Deng Xiaoping let the people get rich; the third generation leadership, with Jiang Zemin at its core, will enable China to become a strong country*« (Zhang Wannian 1997, zitiert in: Scobell 2000, S. 1).

verfolgt, etwa durch die 2004 gegründeten Konfuzius-Institute (Leipziger Volkszeitung 2018). Dies lässt sich wie im Falle der ökonomischen Zielsetzungen am elften Fünfjahresplans von 2005 festmachen, in dem erstmals Instrumente auswärtiger Kulturpolitik Chinas benannt wurden. Diese Bestrebungen stehen nicht alle direkt mit einzelnen Cyberoperationen in Verbindung. Jedoch lässt sich plausibilisieren, dass die proaktivere Verfolgung chinesischer Interessen auf außen- und sicherheitspolitischer Ebene zwischen 2003 und 2012 mithilfe von Cyberspionageoperationen, durchgeführt auch durch Proxys, forciert wurde.

Für die Erklärung der AV II kann unter Hu Jintao keine eindeutige Präferenz bezüglich eines bestimmten Akteurs bei der Anleitung der Cyberproxys festgestellt werden. So wurden von 2003 bis 2012 jeweils zehn Proxyoperationen der PLA (inkl. APT1) sowie dem MSS zugesprochen. Auch deren Operationsprofil in besagtem Zeitraum kann nur als wenig distinkt voneinander beschrieben werden. Sowohl PLA- als auch MSS-Proxys waren in die vorherrschende Praxis der Wirtschaftsspionage gegenüber demokratischen Ländern involviert, gleiches gilt für Cyberspionage gegenüber regionalen Nachbarn. Für APT1 kann in diesem Zeitraum jedoch ein klarer Fokus auf wirtschaftliche Spionage gegenüber den USA ausgemacht werden, was das Interesse Chinas in dieser frühen Phase des Cyberkonfliktaustrages unterstreicht, zum weltweiten Technologieführer aufzuholen. Dass es sich hierbei um einen militärischen Akteur handelte, deutet auf ein damals noch wenig ausdifferenziertes Aufgabenprofil der Hacker, jedoch wahrscheinlicher auf eine Art Militarisierung der Wirtschaftsspionage hin. Die Involvierung der PLA spricht dafür, dass die wirtschaftlichen Zielsetzungen der KPC direkt mit der nationalen Sicherheit und Verteidigung und somit der Regimesicherheit verknüpft wurden. Konkret schuf wirtschaftliches Wachstum die finanzielle Grundlage für ein ausgeweitetes Verteidigungsbudget und somit die angestrebte Modernisierung der Streitkräfte (DoD 2020, S. 5). Dies entspricht auch der Darstellung der KPC, dass ihre Cyberspionageoperationen nicht etwa aus ökonomischen, sondern aus sicherheitspolitischen Erwägungen heraus interpretiert werden müssten, da das Regime die beiden Sphären kaum voneinander trenne. Kaum ein Fall verdeutlicht dies so gut wie die chinesische Cyberspionage gegen das US-Rüstungsunternehmen Lockheed Martin mit dem Diebstahl der Konstruktionspläne des Kampfjets F-35 aus dem Jahr 2007. Verantwortlich gemacht wurde die PLA, deren Hacker-Gruppierungen bislang einen vor allem ökonomischen Aktionsfokus aufgewiesen hatten. Die Sektoren der nationalen Sicherheit und Wirtschaft verschwommen immer mehr, so auch ideelle und kommerzielle Interessen der KPC. Der Diebstahl der Konstruktionspläne diente somit nicht nur ökonomischen Interessen, sondern auch dem Bestreben nach wirtschaftlicher Modernisierung, schwächte jedoch gleichzeitig die relativen Marktvorteile US-amerikanischer Wirtschaftsunternehmen.

Aus republikanischer Perspektive könnte ein weiterer Grund für dieses ungewöhnliche inhaltliche Portfolio der PLA auch die Schwäche Hus gegenüber dem Militär gewesen sein. Dies veranlasste ihn im April 2009 schließlich dazu, die PLA öffentlich zu kritisieren und deren Rückbesinnung auf sozialistische chinesische Werte im Gegensatz zu nationalistischen Bestrebungen zu fordern. Hierdurch versuchte er, mit seinem Vorgänger Jiang affiliierten PLA-Hardlinern zuvorzukommen, die vor allem gegenüber den USA, aber auch Taiwan sowie im Südchinesischen Meer ein aggressiveres Auftreten Chinas forderten (Duchâtel 2009, S. 110). Deren nationalistisch motivierte Interessensdurchset-

zung widersprach jedoch den ökonomischen Interessen hochrangiger KPC-Eliten, die sowohl mit den USA als auch Taiwan bedeutende Geschäftsbeziehungen zu dieser Zeit pflegten (Duchâtel 2009, S. 111).

Die chinesischen Cyberoperationen der PLA unter Hu reflektieren diesen Interessenswiderspruch, gleichzeitig jedoch auch dessen Ausbalancieren: So wurden keine disruptiven Cyberoperationen gegen taiwanesische oder US-Ziele berichtet, wie es vermutlich im Sinne mancher PLA-Offiziere gewesen wäre, trotz der im Rahmen der Analyse der KV beschriebenen PLA-Doktrinen zum offensiven Cyberkonfliktaustrag wie der »*Integrated Network Electronic Warfare*«-Strategie (Krekel 2009, S. 6).

Auch die Kategorie der allgemeinen Konfliktdimension im HD-CY.CON belegt den weniger rein militärischen Einsatz offensiver Cyberoperationen in dieser frühen Phase: Bis 2014 wurden lediglich solche konventionelle Konflikte mit chinesischen Cyberoperationen in Verbindung gebracht, die laut HIIK-Konfliktbarometer gewaltlose Konflikte darstellten. Die Wirkung der IV wird somit durch das in diesem Zeitraum moderate allgemeine Konfliktniveau insofern moderiert, als mit einer Ausnahme keine PLA-Cyberoperationen mit direkt militärischem Bezug verzeichnet werden konnten. Dabei handelte es sich laut einem geleakten Bericht der ›US-China Economic and Security Review Commission‹ um zwei Vorfälle in 2007 und 2008, bei denen Hacker entsprechend chinesischer Militärprotokolle »*used a ground station to interfere with the operation of two US government satellites used for earth observation*« (Branigan und Halliday 2011).[58] Die Kommission schlussfolgerte weiter, dass diese Operationen mutmaßlich dazu gedient hätten, weitere Schwachstellen der US-Satellitensysteme zu identifizieren. Diese Form militärisch geprägter Cyberoperationen kann als eine Art strategische Aufklärung zur Vorbereitung künftiger Angriffe gewertet werden. Die Entwicklung offensiver Cyberangriffsinfrastrukturen erfordert das beständige Sammeln von Informationen über Zielsysteme. Das Anvisieren von Kommunikationssatelliten, über die die Steuerung militärischer Netzwerke erfolgt, stellt ein attraktives Ziel für künftige Cyberangriffe dar, besonders im Kontext bewaffneter Konflikte mit hochgradig vernetzten Streitkräften wie denen der USA (Pavur 2021, S. 51). Dieser Fokus der PLA legt nahe, dass die Durchsetzung der eigenen Interessen in absehbarer Zukunft als potenziell so konfliktiv zu denen der USA eingeschätzt wurden, dass eine militärische Auseinandersetzung aus chinesischer Sicht nicht mehr ausgeschlossen werden konnte.

Aufseiten des MSS stechen besonders ab 2007 längerfristig angelegte Cyberspionageoperationen mutmaßlicher Proxys des Ministeriums heraus. So wurden allein zwischen den Operationsstartjahren 2009 bis 2011 acht MSS-Proxyoperationen im Datensatz verzeichnet, deren berichtete Dauer mindestens fünf Jahre betrug. Dieser Befund indiziert, dass chinesische HackerInnen bereits damals stärker zu längerfristigen Cyberoperationen bereit und in der Lage waren, als 2016 von US-Experten noch suggeriert wurde (vgl. Costello 2016, S. 8). Die überwiegend ökonomisch-militärischen Ziele, wie sie etwa in einer US-Anklageschrift aus 2018 benannt wurden (DoJ 2018c), entsprechen

58 Im HIIK-Konfliktbarometer ist für die beiden Jahre zwar kein Konflikt zwischen China und den USA verzeichnet, dennoch weisen die beiden Cyberoperationen wie beschrieben eine wahrscheinlich militärisch geprägte Zielsetzung auf.

dem Profil des 2007 von Hu eingesetzten MSS-Chefs Geng Huichang, der zuvor Experte im Bereich der internationalen Beziehungen war und dem eine erhebliche Expertise im Bereich der *»Commercial Intelligence«* attestiert wurde (Bodeen 2007). Hu Jintao könnte das MSS somit dazu genutzt haben, seine ökonomischen Interessen auf außenpolitischer Ebene auch im Cyberspace proaktiver zu verfolgen, quasi als eine Art Gegengewicht zur PLA im Bereich der ökonomischen Spionage.

Die KPC unter Xi Jinping

Xi Jinping sah sich bei seiner Amtsübernahme 2012 als Generalsekretär der KPC und 2013 als Staatspräsident mit erheblichen Herausforderungen auf sozio-ökonomischer Ebene konfrontiert: Die Bestrebungen seines Vorgängers, Chinas wirtschaftliche Entwicklung nachhaltiger zu gestalten und die soziale Ungleichheit einzudämmen, hatten wenige Erfolge gezeitigt. Stattdessen war das Ausmaß an Korruption und Elitenbereicherung innerhalb der KPC ungebrochen hoch, die Partei lief Gefahr, ihre historisch legitimierte Bodenhaftung als Garant der Verwirklichung der ›nationalen Erneuerung‹ des Landes zu verlieren. Diesen Entwicklungen entgegnete Xi einen verstärkt personalistischen Politikstil (Shirk 2018) mit Implikationen auf der ideellen sowie vor allem auch republikanischen Ebene. Die Aufhebung der Amtszeitenbeschränkung, die Auswahl getreuer Gefolgsleute in das Ständige Komitee des Politbüros sowie weitere Maßnahmen zur Einschränkung der Interessensdurchsetzungschancen von KPC-Mitgliedern mit abweichenden Meinungen charakterisieren diesen zunehmend exklusiven Herrschaftszugang Xis (ECPR 2017, S. 1). Der zuvor zumindest noch innerhalb der KPC in Teilen vorhandene Transmissionsriemen wurde somit durch Xi immer stärker verkürzt. Anders gesprochen beraubte er potenzielle Vetospieler innerhalb der Partei, etwa Bo Xilai, nach und nach ihrer Verhandlungsmacht. Gleiches gilt für die PLA: So wurde etwa 2017 der damalige PLA-Oberbefehlshaber Fang Fenghui zu einer lebenslangen Gefängnisstrafe wegen Korruption verurteilt, was laut ExpertInnen jedoch eher auf dessen Allianzbildung mit anderen Anhängern Jiangs und deren berichtete Coup-Pläne gegenüber Xi zurückzuführen sei (Tse 2018). Zudem bildete der verstärkte Personenkult um Xi, auch durch die Aufnahme des *»Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era«* in die chinesische Verfassung 2017, in Kombination mit zunehmend nationalistischen Anleihen die Basis für Chinas aggressiveres Auftreten auf internationaler, aber auch domestischer Ebene (Holbig et al. 2017).

Die unter Xi zunehmend auf ihn zugeschnittene Präferenzordnung der KPC wird nun anhand dreier Prinzipien analysiert, die alle drei Ebenen des Liberalismus betreffen.

***»Spiritual Civilisation«*: Parteiendisziplin als Voraussetzung ideeller Interessensdurchsetzung**

Als Erbe seiner Nachfolger musste sich Xi von Beginn seiner Amtszeit an mit der grassierenden Korruption und damit verbundenen sozialen Ungleichheit im Land befassen, trotz der Bemühungen Hus, beiden Entwicklungen entgegenzuwirken (Bhattacharya 2019, S. 249). Durch den technokratischen Diskurs unter Hu kam es ferner zu einer noch größeren Entfremdung zwischen Partei und Volk (Brown und Bērziņa-Čerenkova 2018, S. 327). Die Einheit der Nation und die Position der KPC schienen durch diese beiden Entwicklungen zunehmend gefährdet zu sein:

> »The Party was both privileged, the recipient of an incontestable mandate to rule, but also seeking ways, in a society where its ideological hold was growing more and more elusive, in which it could demonstrate validity to the wider world beyond its membership that was not just based on force, fear, and coercion but something approaching an idea of service and legitimization through performance.« (Brown und Bērziņa-Čerenkova 2018, S. 330)

Die wirtschaftliche Performanz auf der Makroebene reichte als Legitimationsgrundlage nicht mehr aus. Stattdessen musste die Bevölkerung wieder von der kommunistischen Integrität der KPC und ihrer Fähigkeit, materielle sowie immaterielle Güter zum Wohle aller generieren und verteilen zu können, überzeugt werden.[59] Ein Wandel der Interessensdurchsetzungschancen auf der republikanischen Ebene wurde somit zur Voraussetzung der Interessensdurchsetzung der Partei auf ideeller und ökonomischer Ebene sowie ihrer eigenen Position im politischen System.

Um innerhalb der Bevölkerung wieder verstärkte Legimitation zu erzeugen, mussten zunächst Reformen auf der republikanischen Ebene durchgeführt werden. Die Antikorruptionskampagne Xis sollte einer nachhaltigeren Entwicklung den Weg ebnen. Neben den später noch zu behandelnden ökonomischen Maßnahmen wurde dieses Interesse auch durch ideologisches Framing verfolgt. Das Konzept der Transformation Chinas zu einer ›Spiritual Civilization‹ stellte ein Hauptelement dar, um die BürgerInnen nach Jahren ideeller Entfremdung wieder stärker ›auf Kurs zu bringen‹, mit der Einhegung der Korruption als Voraussetzung. Auch wenn das Prinzip bereits seit 1986 von chinesischen Präsidenten als notwendig betont wurde, um der steigenden Dekadenz in Folge marktliberaler Öffnung Herr zu werden (Feng 1998, S. 33), legte kein KPC-Anführer einen solch großen Fokus darauf wie Xi Jinping. Sozialistisch-konfuzianische Werte in marxistisch-kommunistischer Tradition bilden den Grundpfeiler des Prinzips. Konkurrierende Werte- und Glaubenssysteme wie der Islam der Uiguren in der Region Xinjiang oder der tibetische Buddhismus sollen hierdurch ausgemerzt werden, da sie als Gefahr für die aspirierte Einheit der Nation der Han-ChinesInnen gelten (Boehm 2009, S. 74).

Die Interessenskombination aus Korruptionsbekämpfung und gesellschaftlicher Einheit auf Basis sozialistischer Prinzipien kann einige Cyberproxyoperationen chinesischer Hacker ab 2013 hinsichtlich beider AVs erklären (n = 73 von 115). Bis einschließlich 2019 waren in 16 Fällen vier der ›Five Poisons‹ unter den anvisierten Zielen:[60] DemokratieaktivistInnen aus Hongkong, tibetische, uigurische sowie taiwanesische Ziele. Gemeinsam haben diese ihr Gefährdungspotenzial für Chinas nationale Einheit auf kultureller und, daraus resultierend, politischer Ebene. Hongkongs Demokratiebewegung stellt besonders seit dem im Februar 2019 angekündigten nationalen Sicherheitsgesetz den Herrschaftszugang der KPC über die Sonderverwaltungszone zunehmend in Frage und fordert rechtlich zugesicherte Autonomierechte im Rahmen von Protestbewegungen öffentlichkeitswirksam ein (Reuters 2020b). Tibet und die von muslimischen

59 Auf ideeller Ebene wurde dieser Prozess auch als die »*Three Belief Crises*« bezeichnet (Wang 2014, S. 6).

60 In den 16 Fällen war jeweils mindestens eins der vier ›Poisons‹ unter den Zielen.

Uiguren bewohnte Region Xinjiang bedrohen stattdessen aufgrund deren separatistischer und aus chinesischer Sicht extremistischer Tendenzen das Ziel einer ›Spiritual Civilization‹. So werden vor allem die Uiguren als islamistische Terroristen dargestellt, deren Glauben nicht mit der sozialistischen Werteordnung kompatibel sei. Auf analoger Ebene reagierte das Regime speziell unter Xi mit sog. ›Umerziehungslagern‹, die jedoch von westlichen MenschenrechtsaktivistInnen und seit 2021 auch der US-Regierung eher mit Konzentrationslagern verglichen wurden (Wong und Buckley 2021). Zuletzt entzieht sich Taiwan aus chinesischer Sicht schon viel zu lange der Kontrolle der KPC, indem die Ein-China-Politik zunehmend kontestiert wird (Deuber und Krüger 2021).

Das Profil der Ziele entspricht den wahrgenommenen Verwundbarkeiten der KPC gegenüber diesen AkteurInnen: In den sechs Fällen mit Zielen aus Hongkong wurden u.a. die Regierung, dort operierende zivilgesellschaftliche Organisationen sowie die Universität Hongkong ausspioniert. Bereits 2014 hatte es zudem Spekulationen darüber gegeben, ob die chinesische Regierung in großangelegte DDoS-Angriffe auf unabhängige Medien im Zuge der »*Occupy Central*«-Proteste in Hongkong verwickelt war (Olson 2014). Aufgrund der wenig substanziellen Attributionslage erfasst der HD-CY.CON diesen Fall jedoch nicht mit China als ›Initiator-Country‹.

Zwischen 2016 und 2018 wurde in drei Fällen die tibetische Gemeinschaft als Ganzes zum Ziel chinesischer Cyberspionage. Aufseiten der uighurischen Minderheit registriert der Datensatz unter den hier erfassten Cyberproxy-Fällen zwei Spionagekampagnen (2013 und 2017). In fünf Fällen wurden zwischen 2015 und 2018 ferner politische Institutionen wie Ministerien oder Parteien Taiwans anvisiert. Aber auch Unternehmen waren von den Spionageoperationen betroffen.[61]

Im Zuge der Analyse der AV II fällt für das Interesse Xis an der Bekämpfung der KPC-Korruption auf, dass die hiermit kolportierte Umstrukturierung der PLA wohl auch einen Einfluss auf die Zuständigkeiten im Cyberspace hatte. Von 2013 bis 2019 wurden lediglich zehn PLA-Proxyoperationen im Kontrast zu 26 MSS-Proxyoperationen im HD-CY.CON verzeichnet. Wie bereits beschrieben, schien das quantitative Kräfteverhältnis unter Hu noch wesentlich ausgeglichener gewesen zu sein, was der Umstrukturierung der Zuständigkeiten im Cyberspace innerhalb der chinesischen Sicherheitsarchitektur zu entsprechen scheint. Der nach wie vor prävalente Fokus auf Spionageoperationen, gepaart mit der seit 2015 gestärkten Rolle des MSS darin, erklärt auch dessen häufige Kodierung im Datensatz. Demgegenüber konzentrierte sich die PLA im Cyberspace ab 2015 im Rahmen der gegründeten SSF noch stärker auf den Ausbau offensiver Cyberoperationsfähigkeiten mit disruptiver Wirkung und im Rahmen konventioneller Konflikte.

Das bisherige Ausbleiben einer kriegerischen Auseinandersetzung mit Taiwan kann das Fehlen disruptiver Cyberoperationsformen auch unter der Leitung von Xi im Datensatz erklären. Inwiefern jedoch die KPC künftig die Aktivitäten der ›Five Poisons‹ als Gefahr für das Ziel einer ›Spiritual Civilization‹ im chinesischen Geiste einschätzt, könnte auch über eine mögliche Eskalation der Cyberoperationen mitbestimmen und die PLA wieder in den Fokus rücken.

61 Durch den Wahlsieg der stärker nach Unabhängigkeit strebenden Democratic People´s Party 2016 nahm die Bedrohungsperzeption Taiwans durch die KPC noch weiter zu.

Neben Operationen gegen die ›Five Poisons‹ können auch die berichteten Cyberoperationen mutmaßlich chinesischer Hacker mit Militärhintergrund 2012 und 2013 gegen US-JournalistInnen und Medienhäuser wie Bloomberg oder die New York Times durch das Motiv der ›Spiritual Civilization‹ plausibilisiert werden (Perlroth 2013). Deren umfangreiche Recherchen hatten zuvor den immensen Reichtum von Xi-Verbündeten wie dem Premierminister Wen Jiabao sowie Xis eigener Familie öffentlich gemacht (Bloomberg News 2012; Barboza 2012). Die Interessensdurchsetzung amerikanischer Medien kollidierte mit der Präferenzordnung der KPC auf ideeller Ebene, die die Erneuerung des Glaubens der Bevölkerung in die Integrität der Partei vorsah. Cyberoperationen wurden somit eingesetzt, um diese asymmetrische Verwundbarkeit zu reduzieren und möglichen weiteren Investigativrecherchen durch eine frühzeitige Kenntnis hierüber zuvorzukommen.

Ein weiterer Fall, in dem die eigene Verwundbarkeit auf ideeller Ebene versucht wurde zu manipulieren, war die großangelegte DDoS-Operation gegen die US-Entwicklerplattform GitHub 2015 (Stone 2015a). Deren Bereitstellung von Technologien zur Umgehung der chinesischen Zensurmaßnahmen kollidierte aus Sicht der KPC mit dem Ziel der ›Spiritual Civilization‹. Da das Stören der Funktionsweise der Plattform lediglich temporärer Natur sein konnte, schien hiermit eine doppelte Signaling-Funktion an US-Technologiekonzerne und die eigenen BürgerInnen verbunden gewesen zu sein: Dass Erstere auf technischer Ebene selbst verwundbar sind und Letztere aufgrund der gegebenen Allmacht chinesischer Zensoren im Internet stets vom ausländischen Diskurs abgeschnitten werden können.

Zuletzt gilt es den Einfluss der IV in diesem konkreten Fall genauer zu beurteilen: Alle elf für China verzeichneten Cyberproxyoperationen mit gewaltsamer konventioneller Komponente fielen in die Zeit der Präsidentschaft Xis. Jedoch war keine dieser Cyberoperationen disruptiver Natur und somit auch nicht mit physischen Schäden verbunden. Betroffen waren viermal Ziele in Hongkong, dreimal in Tibet, zudem jeweils einmal Entitäten aus Vietnam, der Mongolei, Xinjiang sowie den am Konflikt um das Südchinesische Meer beteiligten Ländern. Das allgemeine Konfliktniveau überstieg jedoch nie das Level 3 der HIIK-Skala, was für eine ›Violent Crisis‹ und noch keinen Krieg steht. Hierdurch erklärt sich auch die scheinbar eingeschränkte Erklärungskraft der H2 der IV für China, da für besagte gewaltsame Konflikte, wenn überhaupt, MSS-Proxys im Datensatz attribuiert wurden. Aufgrund der noch niedrigeren Gewaltintensität boten stärker militärisch geprägte Cyberoperationen weniger Nutzen als Spionage, weshalb das MSS und nicht die PLA in der Verantwortung war.

The »Chinese Dream«: **Nationale ›Selbsterneuerung‹ auf außenpolitischer Ebene**

Als zweites Leitinteresse der KPC unter Xi wird das Streben nach nationaler Selbsterneuerung vor allem auf außen- und sicherheitspolitischer Ebene identifiziert.[62] Neben

62 »Beginning in early 1990s, the Party used the new phrase »the great rejuvenation of the Chinese nation« (zhonghua minzu de weida fuxing) as its new mission. By using the word »rejuvenation,« it stressed that the Party's work was to restore China to its former position and glory. The mission of the Party was no longer the realization of communism, having deviated to a more nationalistic objective.« (Wang 2014, S. 6).

der im nachfolgenden Abschnitt genauer behandelten Wiederbelebung historischer Handelsrouten entlang der Seidenstraße liegt es im besonderen Interesse der KPC unter Xi, chinesische Territorialansprüche auf Grundlage historischer Rechtfertigungen proaktiver zu vertreten. Den »*Chinese Dream*« beschrieb Xi 2012 als »*the goal of completing the building of a wealthy, powerful, democratic, civilized, and harmonious socialist modernized nation*« mit 2049, dem 100. Geburtstag der VR als Zieldatum (Xi 2012, zitiert in Cooper, III 2018, S. 1).

Um eine ›powerful‹ Nation zu werden und sich gegenüber Ländern wie den USA auch im militärischen Bereich besser behaupten zu können, setzt die KPC unter Xi Jinping viel daran, den bereits unter Hu begonnenen Weg der Modernisierung der PLA vor allem im Bereich der Seestreitkräfte und darauf stationierter Luftverbände zu forcieren (Wuthnow und Saunders 2017, S. 8). Ein solcher Kapazitätsaufbau entfaltet im Rahmen der maritimen Konflikte der Region eine große Bedeutung. Der Konflikt um das Südchinesische bzw. auch Ostchinesische Meer hat seine Ursprünge in der Zeit nach dem Zweiten Weltkrieg. In den darauffolgenden Jahrzehnten entfachten sich immer wieder Streitigkeiten um verschiedene Inselgruppierungen: Zwischen China und Vietnam um die Paracel-Inseln, zwischen China, Japan und Taiwan um die Senkaku-Inseln sowie zwischen China, Malaysia, Brunei, Taiwan, Vietnam und den Philippinen um die Spratly-Inseln (Mirski 2015). Die teilweise mithilfe archäologischer Beweisführung untermauerte Behauptung, China sei historisch bedingt der rechtmäßige Souverän über die genannten Territorien (PRC Embassy Philippines 2016), steht in direkter Verbindung mit der angestrebten nationalen Selbsterneuerung. Sich etwa gegenüber Japan im Streit um die Senkaku-Inseln zu behaupten, stellt für die KPC ein Mittel dar, um sich im Sinne des ideologischen Narrativs von jahrzehntelanger »*hardship and humiliation*« ehemaliger Kolonialmächte zu befreien (Peters 2017, S. 1302).

Die im Rahmen dieser Territorialkonflikte mit zunehmend nationalistischer Rhetorik verbundene Politik der KPC traf auf große Zustimmung innerhalb der chinesischen Bevölkerung, die ebenfalls irredentistische Haltungen offenbarte (Kleinsteiber 2013; Lim 2016). Auf analoger Ebene schuf die VR speziell ab 2014 Fakten, etwa indem sie die besetzten Spratly-Inseln bis 2016 zu Militärbasen umfunktionierte oder eine ›Air-Defense-Identification-Zone‹ implementierte (Ramadhani 2019, S. 32). Die zunehmend aggressive Regionalpolitik Chinas führte 2016 letztlich zum bereits erwähnten Urteil des Schiedsgerichtes in Den Haag, das im Sinne der Philippinen und somit gegen die VR und dessen ›Nine-Dash Line‹ urteilte. Das immer häufigere Verletzen internationaler Regelungen und Vereinbarungen kann als ein neues Charakteristikum chinesischer Außenpolitik gelten, entgegen der zuvor jahrzehntelang propagierten Demut gegenüber der internationalen Staatengemeinschaft, deren Institutionen und der eigenen Rolle hierin. Cyberproxys dienten hier somit der Interdependenzmanipulation gegenüber der internationalen Gemeinschaft, wurde doch zunehmend konfliktiv zu deren Präferenzordnung(en) agiert.

Es werden jedoch auch diverse Beispiele scheinbarer Deeskalationsbemühungen der VR berichtet. So stimmte China 2017 dem Rahmenwerk für einen ›Code of Conduct‹ (COC) mit den Staaten der Association of Southeast Asian Nations (ASEAN) zu, der jedoch 2020 immer noch nicht final beschlossen war (Hoang 2020). Aufgrund der besonders auch im Rahmen der OBOR-Initiative bestehenden Wirtschaftsinterdependenzen

zwischen den ASEAN-Staaten und China kann dies als eine Art Ausbalancieren der eigenen Interessen auf ideell-nationalistischer sowie ökonomischer Ebene gewertet werden.

Das beschriebene Interesse an einer aggressiveren Verfolgung nationalistischer Interessen in besagten Seekonflikten kann einen erheblichen Teil der verzeichneten Cyberoperationen chinesischer Proxys im Datensatz ab 2013 erklären: In über 30 Fällen wurde mindestens eine Konfliktpartei, oftmals wurden jedoch gleich mehrere Konfliktparteien als Ziele kodiert. Japanische, vietnamesische und philippinische Entitäten wurden jeweils siebenmal, thailändische und taiwanesische Ziele fünfmal sowie malaysische Ziele dreimal für den Zeitraum erfasst.[63] Hauptsächliche Zielsektoren waren die jeweiligen Regierungen sowie Ministerien, politische Parteien, Telekommunikationsanbieter, die Rüstungsbranche, weitere Unternehmen, aber auch JournalistInnen und Universitäten. Dieses Zielprofil entspricht dem chinesischen Interesse nach der noch zu behandelnden wirtschaftlichen Modernisierung, aber eben auch den sicherheitspolitischen Ambitionen in der Region. Die verschiedenen ASEAN-Staaten oder auch am Streitschlichtungsverfahren in Den Haag beteiligte AkteurInnen auszuspionieren, spiegelt die chinesische Präferenz einer verbesserten Verhandlungsposition durch Wissensvorsprung wider. Die chinesischen Cyberspionageoperationen gegenüber südostasiatischen Staaten unter der Führung Xis dienen der Schaffung von Informationsasymmetrien, um auch auf anderen Ebenen die Manipulation von Interdependenzkonstellationen ermöglichen zu können.

Die Analyse der AV II zeigt für die asiatischen Seekonflikte dagegen ein ambivalentes Bild: So sind mit den Gruppierungen Tick und APT30 zwar zwei PLA-Ableger unter den attribuierten Akteuren, gleichzeitig übersteigen die MSS-Operationen gegenüber Staaten der Region diese zahlenmäßig. Die beiden PLA-Operationen starteten 2016 und somit nach der militärischen Strukturreform. Trotz ihres Spionagecharakters können diese somit bewusst als militärisch motivierte Handlungen gewertet werden, d.h. als Vorbereitungen auf künftige Konflikteskalationen auch im Cyberspace. Ein FireEye-Bericht von 2019 indiziert jedoch, dass auch die MSS-geführten Spionageoperationen gegenüber Zielen der Region im Einklang mit analogen Militäroperationen stattfinden können: Darin werden die Spionageoperationen von APT40 (aka Leviathan), einem MSS-Ableger, in direkten Zusammenhang mit der 2016 stattgefundenen Beschlagnahmung eines unbemannten US-Navy-Schiffes seitens der PLA Navy gesetzt (Plan et al. 2019). Seit der Errichtung der SSF 2015 könnten PLA- und MSS-Operationen somit zum Zwecke der übergeordneten Zielerreichung regionaler Dominanz stärker integriert und aufeinander abgestimmt erfolgen.

An dieser Stelle sowie weiteren Stellen tritt zudem die zentrale Bedeutung der USA für die Formulierung und Durchsetzung chinesischer Interessen auf außenpolitischer Ebene zutage: Ein Streitpunkt bezüglich des COC ist die chinesische Forderung, die ASEAN-Staaten sollten sich dazu verpflichten, keine Militärmanöver mit Drittparteien abzuhalten. Aufgrund der sicherheitspolitischen Interdependenzen vieler ASEAN-Staaten mit den USA führte dies zu einer Blockadehaltung (Hoang 2020). Bereits 2011 hatte Präsident Obama mit der Ankündigung des sog. »*Pivot to Asia*« aufseiten Chinas

63 Zudem waren Entitäten aus Indonesien und Brunei unter den Zielen. Ferner wurde in mehreren Fällen generisch »*Southeast Asia*« oder »*South China Sea*« als Receiver-Country kodiert.

Einkreisungsängste hervorgerufen: »*The United States will play a larger and long-term role in shaping this region and its future, by upholding core principles and in close partnership with our allies and friends*« (Obama 2011). Auch wenn Obama dies 2014 zurückwies und den Schutz des internationalen Rechts im Rahmen maritimer Konflikte als Hauptmotivation für das US-Engagement bezeichnete (Maresca 2014), änderte dies nicht viel an der zunehmend konfliktiv wahrgenommenen Interessensverfolgung der USA seitens der KPC in der Region. Teil davon war auch das Freihandelsabkommen Trans-Pacific Partnership (TPP), das Obama zwischen den Staaten der Asia-Pacific Economic Cooperation (APEC) und somit ohne die Beteiligung Chinas unterstützte.

Auch auf militärischer Ebene kam es zumindest verbal zu einem verstärkten Engagement der USA. Letzteres wurde jedoch als ›Feigenblatt‹ bewertet, da die USA selbst nicht zu den entsprechenden finanziellen Anstrengungen bereit schienen, die sie von den Ländern der Region einforderten (Harnisch und Friedrichs 2017, S. 9–10). Unter der Ägide von Donald Trump verschärfte sich dieser Interessenskonflikt, da Trump die amerikanische Interessensdurchsetzung gegenüber der chinesischen zunehmend als Nullsummenspiel darstellte (Shirk 2017, S. 24). Existierende Interdependenzen wurden somit negiert bzw. wurde argumentiert, dass deren Status quo im ausschließlichen Interesse des Gegenübers sei. Beispiele für diese konfliktive China-Politik der Trump-Regierung sind (neben dem Handelskrieg) deren Unterstützung für Taiwan in Form immenser Waffenlieferungen sowie kurz vor der Amtsübernahme von Joe Biden die Aufhebung von Reise- und Kontaktbeschränkungen zwischen US-DiplomatInnen und den taiwanesischen Gegenübern (Shih und Kuo 2021).

Entsprechend dieser zunehmenden Präferenzinkompatibilitäten der beiden Länder bezüglich der südostasiatischen Region waren die USA in vier Fällen zusammen mit mindestens einem Land unter den anvisierten Zielen. Deren Abhängigkeiten von den USA als militärischer Schutzmacht spiegeln sich somit auch in der Zielauswahl chinesischer Proxys wider, um ein möglichst umfassendes Informations- und Lagebild über die geopolitische Situation und Allianzbildung erhalten zu können. Ein mögliches Ziel war und ist hierbei vermutlich, bestehende Interdependenzen zwischen den Parteien zu schwächen und die ASEAN-Staaten stärker auf die eigene Seite zu ziehen. Im Falle der zahlreichen weiteren Spionageoperationen chinesischer Proxys, etwa auf US-Verteidigungsunternehmen, kann ein direkter Nexus zu den asiatischen Territorialkonflikten oftmals nicht hergestellt werden, ist jedoch als Kontextfaktor zugleich nicht immer auszuschließen.

Zuletzt lassen sich auch die sechs gegen Indien verzeichneten Cyberproxyoperationen Chinas zwischen 2013 und 2019 im Kontext dieses Interesses an regionaler Dominanz verorten. Noch kein Gegenstand des Datensatzes, jedoch interessant für die Analyse, sind die 2021 kolportierten Infiltrationen des indischen Energienetzes während der militärischen Auseinandersetzungen der beiden Länder im Sommer 2020. Laut indischen Quellen seien diese für den Stromausfall im Mumbai im Oktober 2020 verantwortlich gewesen (Sanger und Schmall 2021). Dies deutet auf eine verstärkte Integration von Cyber- und Militäroperationen hin, wie sie durch die Gründung des SSF als Ziel ausgegeben wurde.

The »Chinese Dream«: Transformation der internationalen Ordnung durch ökonomische Abhängigkeiten

Ökonomischer Erfolg ist bislang auch unter Xi die Hauptmaxime, um den ›chinesischen Traum‹ einer starken, modernen chinesischen Nation bis 2049 verwirklichen zu können. Interessanterweise propagierte er ökonomische Globalisierung als Mittel der Wahl, um diese nationalistische Zielsetzung erreichen zu können (Bhattacharya 2019, S. 249). Die bereits unter Deng eingeführten Marktöffnungsmaßnahmen, das selbstbewusstere Auftreten Chinas auf internationalem Parkett sowie der Fokus der KPC auf technologische Innovationsfähigkeit unter Hu hatten die Präferenz der Partei für wirtschaftlichen Erfolg chinesischer Prägung entsprechend beeinflusst. Gleichzeitig sahen Xis Vorgänger eine noch weitaus passivere Interessensvertretung Chinas auf außenpolitischer Ebene vor, entsprechend der »*Five Principles of Peaceful Coexistence*«.[64]

Zentral waren auch für Xi das Schaffen neuer Interdependenzen zwischen China und weiteren globalen HandelspartnerInnen sowie das Ausnutzen bestehender Verwundbarkeiten des Gegenübers, um eigene Abhängigkeiten reduzieren zu können. In diese Kategorie fallen das gesteigerte Niveau chinesischer FDIs und Entwicklungshilfen sowie die maßgeblich in den Cyberspace verlagerte Wirtschaftsspionage unter Hu. Xi Jinping wurde somit zu einem Zeitpunkt Generalsekretär der KPC, als sich das Kräfteverhältnis im Wirtschaftsbereich und speziell dem Technologiesektor bereits zu Gunsten Chinas und zu Ungunsten der USA verlagert hatte. Nichtsdestotrotz war das chinesische Wirtschaftssystem nach wie vor von steigenden Interaktionen mit weltweiten HandelspartnerInnen abhängig, um Erfolg zu haben. Somit konnte nationalistischer Protektionismus anderer Länder nicht im chinesischen Interesse liegen, nachdem die im Vergleich weitaus schnellere Erholung von der Wirtschaftskrise 2008 erfolgt war (Shirk 2017, S. 21).

Prägnantester Ausdruck des KPC-Interesses an einer proaktiven Beeinflussung des internationalen Handelssystems, um China in seine angestammte internationale Führungsrolle zu bringen, ist die OBOR-Initiative (Mulvad 2019, S. 452). 2013 von Xi verkündet, sah sie eine Reaktivierung der historischen Handelswege entlang der Seidenstraße vor. Hierzu zählte die Initiierung massiver Infrastruktur- und Investmentprojekte in Ländern von Ostasien bis nach Europa mit jeweils einer Dimension an Land und zu Wasser. Dies betraf den Ausbau von Energiepipelines, Bahnschienen, Straßen sowie Flughäfen und Häfen, etwa in den früheren Sowjetrepubliken, aber auch in Südostasien (Chatzky 2020).

Im Zuge der OBOR-Initiative wurden zudem immense Kredite an Entwicklungsländer gewährt, die ihre Aufträge für Großprojekte seitdem oftmals an chinesische Firmen vergeben. Die OBOR-Initiative verbindet somit die ökonomischen Interessen der KPC mit ihren Präferenzen für eine proaktivere Außen- und Sicherheitspolitik, speziell im asiatischen Raum. Gleichzeitig bemüht sich das Regime, die eigene Interessensdurchsetzung als eine ›Win-win‹-Situation und sich selbst als großzügigen Produzenten öffentlicher Güter darzustellen (Cronin 2021). Im Oktober 2018 veröffentlichte Xi ein Buch, in dem er das chinesische Ziel des Aufbaus einer »*Community of Common Destiny*« erklärte. Hierfür propagierte er im Vergleich zu seinen Vorgängern eine weitaus proaktivere,

---

64 »*Mutual respect for territorial integrity and sovereignty, mutual non-aggression, mutual non-interference in internal affairs, equality and cooperation, and peaceful coexistence*« (Tobin 2018, S. 155).

sogar schon führende Rolle Chinas bei der aus seiner Sicht notwendigen Reform des globalen Governance-Systems (Tobin 2018, S. 156). Daraus resultierend bezeichneten KritikerInnen aus den USA, aber auch aus Asien, das OBOR-Projekt als eine Art ›Trojanisches Pferd‹: Die politisch-militärische Machtexpansion der KPC fände unter dem Deckmantel wirtschaftlicher Initiativen statt (Lee 2018).

Im Rahmen seiner Reden vor der UN-Generalversammlung 2015 und 2017 verdeutlichte Xi implizit das Bestreben der KPC, das bestehende internationale System nach eigenem Gusto umzuformen. So sollte dieses nicht durch eine Parallelordnung ersetzt werden, sondern sich vielmehr das überlegene Modell Chinas in den zentralen Sektoren der Politik, Sicherheit und Entwicklung zu eigen machen und somit dem Land seine angestammte Führungsposition verleihen. Chinas inhärentes Streben nach friedvoller Entwicklung, dessen nationaler Erfolgspfad hin zur größten Volkswirtschaft der Welt sowie dessen multilaterale Gesinnung hob Xi vermutlich in direkter Abgrenzung zu den USA unter Donald Trump hervor. Gleiches gilt für die zu vermeidende »*Thucydides Trap*«, einer offensichtlichen Anspielung auf eskalatorische Dynamiken unter dessen Ägide gegenüber China als aufstrebender Macht (PRC Embassy Iraq 2017).

Chinas Cyberoperationen ab 2013 können durch das Interesse Xis an einer wirtschaftlich ermöglichten Transformation des internationalen Systems nach chinesischem Vorbild in erheblichem Ausmaß plausibilisiert werden. Als nach wie vor bestehende Grundpfeiler des chinesischen Cyberkonfliktaustrages fungierten die auch unter Xi in erheblichem Umfang durchgeführten Cyberspionageoperationen mit sowohl ökonomischer als auch politisch-militärischer Prägung. Die USA waren wie zuvor das Hauptziel mit aufsehenerregenden Vorfällen gegen politische Institutionen. Beispiele sind der OPM-Hack 2015 sowie zahlreiche Hacks gegen US-Unternehmen (z.B. Anthem und Marriott 2015). Ab 2013 waren in 24 von 73 untersuchten Proxyoperationen US-AkteurInnen unter den anvisierten Zielen, somit in jedem dritten Fall. Dies entspricht dem exponierten Herrschaftszugang der USA auf internationaler Ebene, ferner in den Bereichen der Politik, Sicherheit und Wirtschaft, aber auch dem Wissenschafts- sowie Kultursektor.

Chinas Interesse nach Führung in diesen Sektoren spiegelt sich in einem ›Abarbeiten‹ an den US-Verwundbarkeiten wider. Für die Dyade China-USA gestaltete sich die von Xi proklamierte Win-win-Situation aufgrund der steigenden Spannungen seit Donald Trumps Amtsübernahme zunehmend zu einem Nullsummenspiel. Die eigene Interessensdurchsetzung wurde somit immer stärker von der Nichtdurchsetzung der Interessen des Gegenübers abhängig gemacht.

Im Bereich der Wirtschaftsspionage führte dieses konsequente Ausnutzen des umfassenden Angriffsvektors im Cyberspace von US-Unternehmen und US-Institutionen jedoch bereits unter Barack Obama zu einem erstmaligen, wenn auch nur zeitweiligen Umdenken der KPC. Aufseiten der USA erhöhte sich in Folge der zahlreichen Spionageoperationen der politische Druck so groß, dass sie 2014 die erste Anklage gegen ausländische Hacker aufgrund von Cyberspionageaktivitäten verhängten. Konkret betroffen waren APT1 und deren Diebstahl geistigen Eigentums von US-Unternehmen im Zeitraum von 2006 bis 2014 (DoJ 2014b). Die chinesische Interessensdurchsetzung auf ökonomischer Ebene hatte somit ein für die USA nicht mehr hinnehmbares Konfliktniveau erreicht. 2015 stimmte die KPC nach erheblichem Druck der Obama-

Administration schließlich einem Abkommen zu, in dem sich beide Länder u.a. darüber verständigten, keine Cyberspionageoperationen mehr gegeneinander auszuführen. In der Folge attestierten US-Unternehmen zumindest für das Jahr 2016 einen deutlichen Rückgang chinesischer Cyberspionage, was sich auch im HD-CY.CON widerspiegelt. Von US-Seite wurde dies jedoch auch auf einen möglichen Anstieg der Sophistiziertheit chinesischer Operationen zurückgeführt (Segal 2016).

Ab 2017 kam es aufgrund der gestiegenen Spannungen im Handelsstreit mit der Trump-Administration wieder zu einer zahlenmäßigen Normalisierung der chinesischen Spionageoperationen gegen US-Unternehmen. Hinsichtlich der Ausprägung der AV II stellten amerikanische IT-Unternehmen jedoch gleichsam eine Veränderung fest: So wurde in Folge der militärischen Umstrukturierung nunmehr hauptsächlich das MSS für diese Formen von Cyberspionage verantwortlich gemacht (Kania und Costello 2018, S. 107). Auch dies bekräftigen die Daten des HD-CY.CON, da (zumindest aufseiten der hier untersuchten Proxyoperationen Chinas) ab 2017 lediglich MSS-Gruppierungen in Fällen mit US-Zielen attribuiert wurden.[65]

Entgegen der Vorhersage des Unternehmens FireEye aus 2016, chinesische Cyberoperationen würden in Zukunft stärker zentralisiert, besser vor kriminellem Missbrauch geschützt und nicht mehr seitens wenig kontrollierter AkteurInnen erfolgen (FireEye 2016, S. 5), schien jedoch genau dies zunehmend ab 2016 der Fall gewesen zu sein. Dies indizieren zumindest die diversen US-Indictments gegen MSS-Proxys wie APT3, APT10 und APT40 und APT41, die wie beschrieben mit Technologieunternehmen in Verbindung stehen. Gleichzeitig legt das für APT41 berichtete Moonlighting nahe, dass der Missbrauch von Staatsressourcen eben nicht konsequent unterbunden werden konnte.

Neben den USA sind weitere Zielländer ab 2013 den wirtschaftlich-politischen Bestrebungen der KPC im Rahmen der OBOR-Initiative zuzuordnen. Hierzu zählen die zahlreichen Operationen gegen Länder wie Myanmar, Singapur, Thailand, Vietnam, Kambodscha, die Philippinen, Russland, Belarus, die Türkei sowie die Mongolei vor, während oder nach dem jeweiligen Beitritt des Landes zur OBOR-Initiative.

Aufgrund ihrer zeitlichen Einordnung im Jahr 2020 nicht im Untersuchungssample enthalten, für diesen Abschnitt jedoch ebenfalls relevant, ist die Spionageoperation der chinesischen APT ›Bronze President‹ gegen die Afrikanische Union (AU) Anfang 2020 (Satter 2020): Der afrikanische Kontinent wurde besonders durch OBOR zunehmend zur chinesischen Einflusssphäre und somit gleichzeitig zum Konfliktgegenstand chinesischer und amerikanischer Interessensvertretungen. Direkt mit OBOR verbunden ist auch der Streit um die chinesische Rolle beim Aufbau weltweiter 5-G-Netzwerke, was vor allem seitens der Trump-Administration als Versuch Chinas dargestellt wurde, die anderen Länder auch auf telekommunikationstechnischer Ebene von sich abhängig zu machen und gleichzeitig auszuspionieren. Auch deshalb entbrannte in der Folge ein Wettstreit zwischen US-Unternehmen und ihren chinesischen Pendants um die Akquise von IT-Infrastrukturprojekten in Afrika (Woo und Wexler 2021). Der Spionagevorfall gegen die AU kann somit als Versuch Chinas gewertet werden, im Wettstreit um die Be-

65 Hierbei handelte es sich um den 2017 stattgefundenen Hack gegen das Finanzdienstleistungsunternehmen Equifax, wofür 2020 vier PLA-Offiziere von den USA angeklagt wurden (DoJ 2020a).

einflussung regionaler Interdependenzen auf technologischer Ebene einen möglichen Vorteil gegenüber den USA zu erhalten.

Technologie-Magnaten als VetospielerInnen?

Abschließend soll die Rolle chinesischer Technologie-Magnaten diskutiert werden: Besaßen diese bislang von der KPC signifikant abweichende Interessen, und falls ja, übten diese einen Einfluss auf den chinesischen Cyberkonfliktaustrag aus?

Im Verbund mit weiteren liberal gesinnten AkteurInnen aus Medien und Wissenschaft vertraten chinesische EntrepreneurInnen in der ersten Dekade des 21. Jahrhunderts den Ansatz eines starken Staates, der in sozial-demokratischer Prägung Innovationen fördert, wofür jedoch eine Demokratisierung des KPC-Systems notwendig sei (Zheng und Tok 2007, S. 11). Im Zuge der Erfolge chinesischer Technologiekonzerne, allen voran Huawei sowie Alibaba, äußerten deren Führungen immer wieder Kritik an Maßnahmen der KPC unter Xi. Ein Beispiel hierfür ist die 2015 erlassene, jedoch im Zuge von internationalem Protest wieder aufgehobene Bestimmung des MPS, dass ausländische IT-Unternehmen chinesischen Banken ihren Quellcode zur Verfügung stellen müssten, was laut damaligem Huawei-Chef Eric Xu den eigenen Cybersicherheitsinteressen Chinas entgegenstehen würde (Austin 2015). Trotz dieser punktuellen Kritik am Vorgehen der Partei werden speziell Huawei enge Verbindungen zum Regime attestiert, was sich in Form von technologisch-operativer Kooperation äußert, ähnlich der Instrumentalisierung unbekannterer IT-Firmen und deren HackerInnen entsprechend der US-Anklageschriften (Balding 2019; Corera 2020). Im Gegensatz zu Huawei, das nach wie vor bedingungslosen Rückhalt der KPC zu genießen scheint, kam es jedoch 2020 zu einer Art Rundumschlag gegen die ›Consumer-Internet-Tech‹: Firmen wie Alibaba, Tencent und Baidu förderten keine Digitalisierung im Sinne der chinesischen ›National Industrial Policy‹, sondern primär zu Unterhaltungszwecken. Der Grund hierfür könnte sein, dass Unternehmen wie Huawei durch ihr immenses Investment in Künstliche Intelligenz sowie die von China lange Zeit vernachlässigte Halbleiterproduktion aus Sicht der KPC nachhaltige Technologiefirmen darstellen, im Gegensatz zu Firmen wie Tencent mit ihren Unterhaltungs-Apps (Smith 2021). Der Grundsatz, dass chinesische Technologieunternehmen an der Herrschaft teilhaben dürfen, solange ihre Interessen nicht denen der KPC entgegenstehen, spiegelt sich auch in einem im HD-CY.CON erfassten Vorfall aus 2017 wider: Dabei wurde die Webseite des Hudson Institutes von mutmaßlich chinesischen Hackern blockiert, nachdem es eigentlich einen chinesischen Tycoon im Exil als Sprecher bei einer Veranstaltung präsentieren sollte (Wen 2017).

Der KPC ist es somit bislang gelungen, die einheimischen Technologieunternehmen zu keinen signifikanten Vetospielern im System werden zu lassen, bzw. im Falle einer Entwicklung in diese Richtung entsprechende Gegenmaßnahmen auf beiden Konfliktebenen zu unternehmen. Aufgrund ihres monopolistischen Herrschaftszugangs schaffte es die KPC auch gegenüber der nationalen Wirtschaftselite, die Interdependenzvulnerabilitäten zum eigenen Vorteil auszugestalten. Dass sie diesen Weg der verstärkten Kontrolle über ihre ›Global Tech-Player‹ fortsetzen wird, deutete sich im Oktober 2021 an: Ein für November 2021 angekündigtes Gesetz schreibt Unternehmen Regeln und Beschränkungen für das Speichern von Daten von chinesischen BürgerInnen vor, der Zugriff staatlicher Behörden wurde dagegen nicht eingeschränkt (Associated Press 2021).

Konkret geht es dabei wohl um die Risikominimierung ungewollter Datenleaks. Welchen Nutzen ausländische AkteurInnen aus persönlichen Daten chinesischer BürgerInnen ziehen könnten, dürfte der KPC nur allzu bewusst sein.

Eine weitere Gruppierung, die bereits früh unter Xis Führung in den Fokus staatlicher Restriktionsmaßnahmen kam, war die 2016 noch bestehende ›White-Hat‹-Community‹ in China. Deren Aushängeschild Wooyun.org, eine Plattform zur Meldung von Sicherheitslücken durch HackerInnen und IT-ExpertInnen, wurde 2016 mutmaßlich durch staatliche Behörden abgeschaltet (The Wall Street Journal 2016).

Die zentralen Erkenntnisse der chinesischen Fallstudie werden im Anschluss an die Analyse russischer Cyberproxy-Strategien nochmals mit diesen verglichen und gemäß den aufgestellten Hypothesen abschließend eingeordnet.

5.4 Autokratisches Fallbeispiel II: Russland

> »We live in a wondrous time, in which the strong is weak because of his scruples and the weak grows strong because of his audacity.«
> *Otto von Bismarck, zitiert in Tsygankov (2019)*

Eine vergleichende Studie über Cyberkonflikt-Austragungsmuster autokratischer Staaten und insbesondere deren Inkorporierung sog. Stellvertreter scheint für Russland als Rechtsnachfolgesubjekt der Sowjetunion passend zu sein. Die außerhalb des Untersuchungszeitraums der Arbeit angesiedelte Operation ›Moonlight Maze‹ von 1998 demonstrierte zum ersten Mal das Potenzial russischer Geheimdienst- und Spionageaktivitäten im zunehmend politische Aufmerksamkeit erfahrenden Cyberspace (Geers et al. 2014, S. 2). Auch auf institutioneller Ebene zeigte sich der Kreml bereits seit den Anfängen der Debatte um eine völkerrechtliche Adressierung des Cyberspace als Konfliktaustragungsraum proaktiv und propagierte bereits 1998 (bis 2010 erfolglos) das erste Mal einen Resolutionsentwurf bezüglich der *»Developments in the field of information and telecommunications in the context of security«* (Maurer 2011). Für den zu untersuchenden Cyberproxy-Gebrauch noch entscheidender ist jedoch die russische Prävalenz für analoge Proxy-Strategien, die auch heute noch ein großes Interesse in der politikwissenschaftlichen Forschendengemeinde weckt (Marshall 2016; Rondeaux 2019; Rauta 2020).

5.4.1 Russische Cyberproxy-Operationen (2000–2019): Wer macht was?

> »Hackers are the same [as artists; Anmerkung der Autorin]. They wake up in the morning, they read about some developments in international affairs, and if they have a patriotic mindset, then they try to make their own contribution the way they consider right into the fight against those who have bad things to say about Russia.«
> *Wladimir Putin, zitiert in Radio Free Europe (2017)*

Wie bereits in den Tabellen 9 und 10 dargestellt, umfasst der HD-CY.CON-Datensatz für die Operationsstart-Jahre 2000 bis 2019 zum Zeitpunkt der Analyse 59 attribuierte russische Proxy-Operationen sowie 37 Vorfälle, die allgemein/direktstaatlich Russland zugesprochen wurden. Zu keiner dieser Operationen bekannte sich der Kreml; dessen teilweise wohl bewusst provokanter Umgang mit entsprechenden Vorwürfen veranschaulicht das obere Zitat Putins.

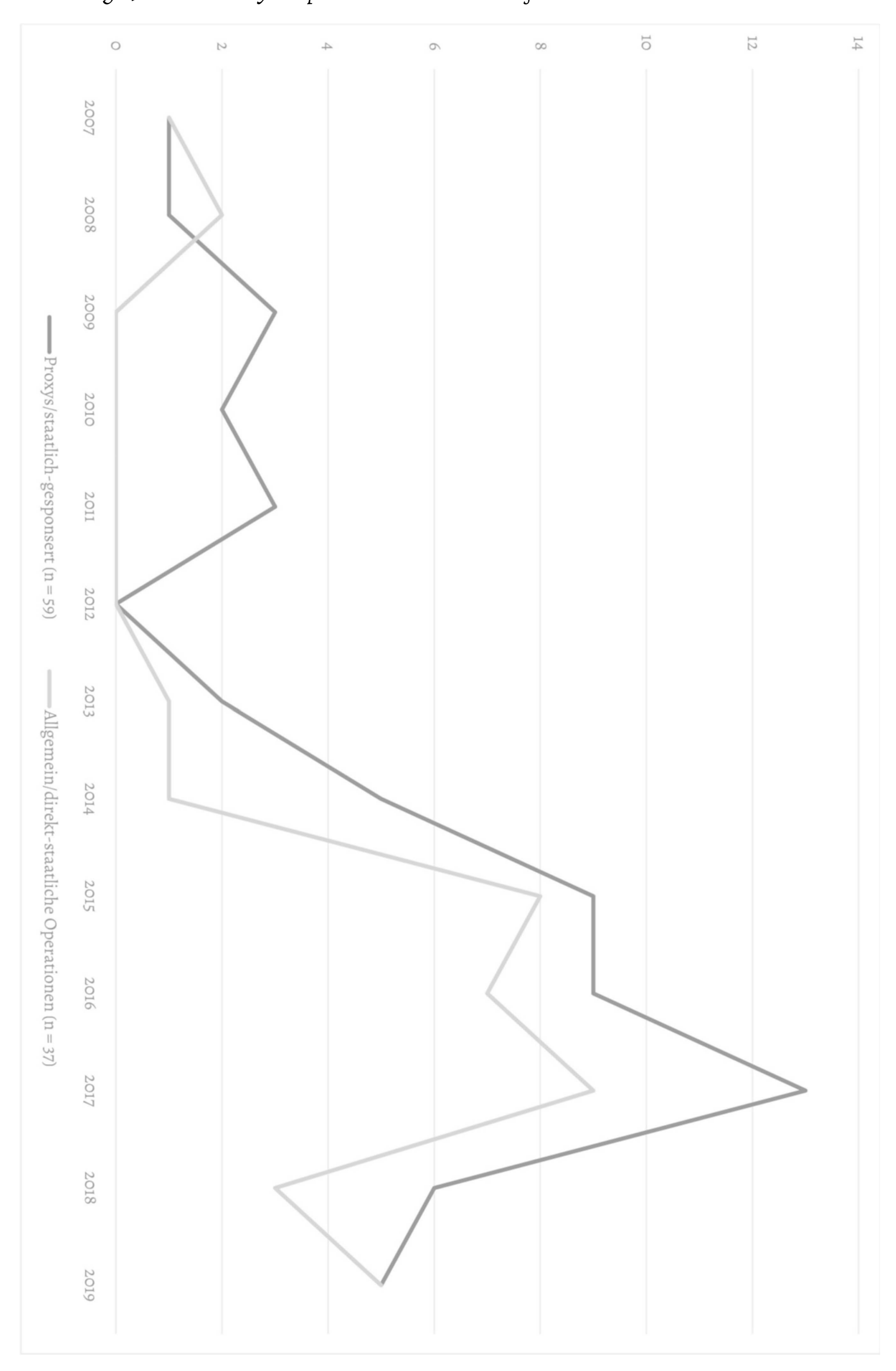
5.4.1.1 Russische Cyberproxy-Funktionen auf Grundlage des HD-CY.CON

Bei der Betrachtung der russischen Cyberoperationen mit attribuierter staatlicher Beteiligung im Zeitverlauf (Abbildung 29) ergeben sich folgende Befunde: Aufgrund der technologischen Pfadabhängigkeit Russlands nach dem Zerfall der Sowjetunion sowie der erwähnten Demonstration staatlicher Cyberoperations-Kapazitäten Ende des 20. Jahrhunderts (Operation Moonlight Maze) ist für russische Cyberproxy-Operationen weniger von einer technischen Erfüllungsgehilfen-Funktion auszugehen. Der Zeitverlauf der Proxy-Operationen lässt stattdessen vermuten, dass Russland vor 2015 und somit der gewaltsamen Eskalation des Ukraine-Konflikts direktstaatliche Cyberoperationen eher gezielt und selektiv einsetzte, bzw. in dieser Phase besonders auf Proxys setzte. Vor allem für den Zeitraum von 2008 bis 2011 könnte hierfür besonders das ambivalente, auf Harmonisierung ausgerichtete amerikanisch-russische Verhältnis verantwortlich gewesen sein, was Bestandteil der Analyse der UV sein wird. Die damals noch als glaubhafter einzustufende Verantwortungszurückweisung durch die Instrumentalisierung russischer Cyberproxys könnte in dieser Phase insbesondere Cyberspionage gegen die USA und ihre Verbündeten ermöglicht haben, ohne jedoch die teilweise erfolgreiche Sicherheitskooperation im analogen Bereich zu gefährden (Stichwort »*Reset*«; Deyermond 2013).

Ab 2015 korrespondierten die Zu- und Abnahme staatlich gesponserter sowie allgemeiner/direktstaatlicher Cyber-Operationen mit russischem Ursprung weitgehend miteinander, im Unterschied zu den chinesischen Cyberoperationen. Daher wird grundlegend davon ausgegangen, dass Cyberproxys für Russland zur Verschleierung der eigenen Cyberoperationen und der eigenen Verantwortlichkeit sowie womöglich auch zur internen Überwachung von Regimeeliten eingesetzt werden, jedoch nicht aus bloßem Mangel an staatlichen Alternativen.

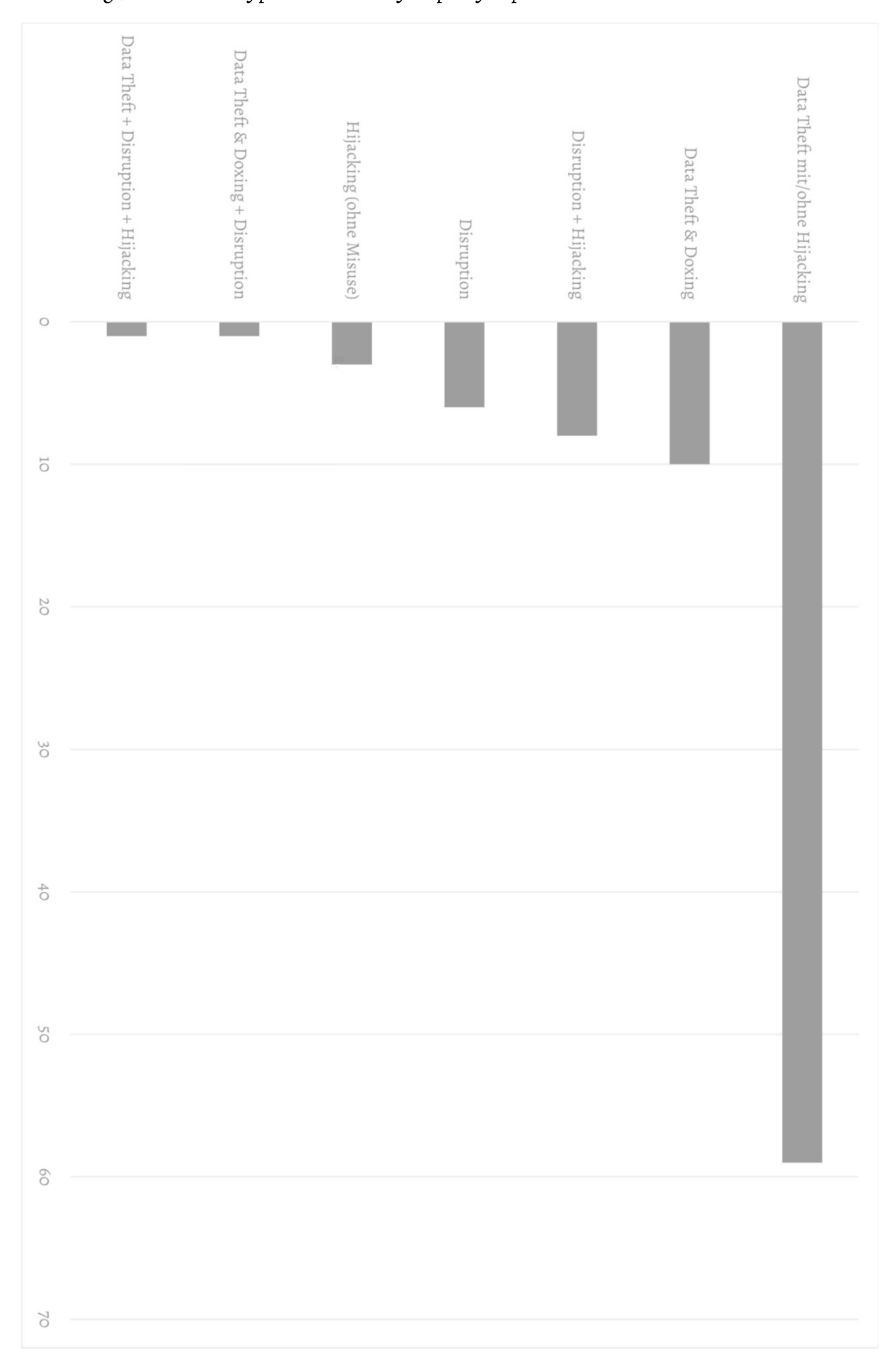
Im Datensatz waren für 67 der 96 erfassten Cyberoperationen mit attribuierter Involvierung des russischen Staates (Initiator-Categorys 1, 2 und 2,1) allein vier Gruppierungen/APTs verantwortlich: Fancy Bear aka APT28, Cozy Bear aka APT29, Sandworm aka Voodoo Bear sowie Turla aka Snake/Waterbug. Hinzu kommen insgesamt sechs Operationen der Gruppierungen Gamaredon Group und Energetic Bear aka Dragonfly, die ebenfalls in beide Kategorien fallen. Dementsprechend beziehen sich alle nachfolgenden Zahlen und Statistiken auf die 59 Fälle mit russischer Proxy-Attribution plus der 29 allgemein/direktstaatlich attribuierten Fälle der genannten sechs Proxygruppierungen (n = 88). Dies deutet bereits auf einen grundlegenden Unterschied zu China hin: Russische Cyberoperationen verteilen sich auf deutlich weniger Gruppierungen, die entsprechend der Attributionslage zudem eine ambivalentere, diffusere Beziehung zu staatlichen Stellen aufzuweisen scheinen als die ca. 37 als Proxys identifizierten chinesischen Gruppierungen.

Abbildung 29: Russische Cyberoperationen im Zeitverlauf



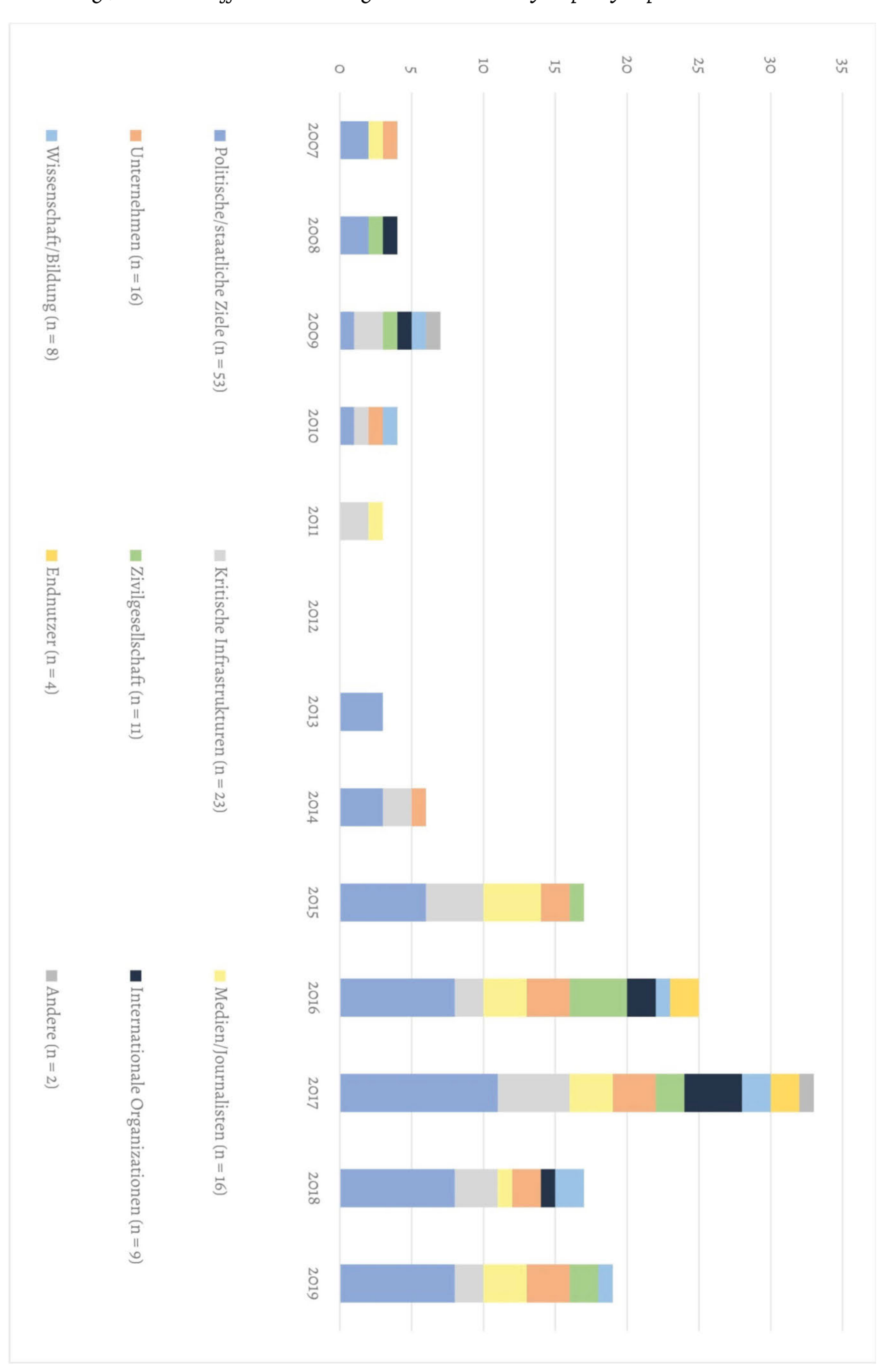
(Eigene Darstellung auf Basis des HD-CY.CON)

Abbildung 30: Incident-Types russischer Cyberproxy-Operationen



(Eigene Darstellung auf Basis des HD-CY.CON)

Abbildung 31: Die betroffenen Ziel-Kategorien russischer Cyberproxy-Operationen



(Eigene Darstellung auf Basis des HD-CY.CON)

Für die 88 Cyberproxyoperationen dominierte Data Theft als kodierter Incident-Type im Untersuchungszeitraum mit 59 entsprechenden Cyberoperationen (Abbildung 30). Operationen, die (auch) disruptivere Komponenten wie Disruption oder Doxing beinhalteten, machten mit 26 erfassten Fällen somit 29,5 Prozent der hier untersuchten 88 Vorfälle aus.[66] Dabei kam es im Gegensatz zu den chinesischen Cyberproxy-Operationen zu einer Vielzahl an Incident-Type-Variationen. Welche Proxy-Funktionen damit jeweils verbunden waren, gilt es durch die Betrachtung der anvisierten Zieltypen und -länder weiter einzugrenzen.

In 53 der 88 untersuchten Operationen russischer Cyberproxys waren politische/staatliche AkteurInnen alleinige oder eines der anvisierten Ziele (Abbildung 31). Verantwortlich ist hierfür wie bei China in erster Linie der prävalente Operationstyp der Cyberspionage. In zehn der (reinen) Spionage-Fälle gegen (u.a.) politische/staatliche Ziele handelte es sich um Operationen mit zugrunde liegendem konventionellen Konflikt. Zwei hiervon wurden im entsprechenden Jahr seitens des HIIK als gewaltsam eingestuft und visierten gezielt auch militärische AkteurInnen an, was somit auf militärstrategische Cyberspionage hindeutet.[67] Nichtsdestotrotz wurden politische/staatliche AkteurInnen vonseiten russischer Proxys zudem in 12 der 26 (u.a.) disruptiven Cyberoperationen anvisiert. Somit wurden sie nicht nur zur politischen Cyberspionage, sondern auch zur Schwächung politischer Gegner mit (drei von 12 Fällen) sowie ohne (neun von 12 Fällen) affiliiertem gewaltsamen Konflikt eingesetzt. Hinzu kommt, dass in vier der 26 disruptiven Vorfälle auch supranationale/internationale Organisationen, etwa die WADA, unter den Opfern waren. Somit kann auch für die Proxy-Funktion der Schwächung (demokratischer) internationaler Organisationen Evidenz auf Grundlage des Datensatzes gefunden werden. Gleiches gilt für die Schwächung demokratischer Werte im Allgemeinen: So wurden in elf von 26 Fällen mit Doxing und/oder Disruption als kodierten Incident-Types auch zivilgesellschaftliche AkteurInnen, etwa 2015 die Open Society Foundation (OSF), oder JournalistInnen/Medien-VertreterInnen, allen voran TV5 Monde 2015, zum Ziel russischer Proxy-Operationen.

Unter den 23 Fällen gegen kritische Infrastrukturen waren sieben Cyberspionage-Operationen gegen den Energie- und vier gegen den Verteidigungssektor gerichtet. Daher kann grundlegend auch die Funktion der militärtechnologischen Cyberspionage dem Portfolio russischer Cyberproxys zugesprochen werden. Die Spionage-Akte gegen den Energiesektor ohne verzeichnete Disruptionen sind schwieriger zu bewerten: Hierbei könnte es sich um vorbereitende Aufklärungshandlungen für mögliche Sabotage-Akte in vor allem gewaltsamen konventionellen Konflikten (z.B. Verwendung der Grey-Energy-Malware gegenüber der Ukraine 2015) gehandelt haben. Möglicherweise stellten

66 Doxing wird dabei als disruptiv auf hauptsächlich psychologischer, reputativer oder sozialer Ebene verstanden, im Gegensatz zu technischen/physischen Schäden (Agrafiotis et al. 2018).

67 Ein aufsehenerregender Fall hierbei war die Implantierung einer Malware in eine vom ukrainischen Militär genutzte App, mit deren Hilfe der Standpunkt der NutzerInnen vermutlich lokalisiert werden konnte. Die US-Firma CrowdStrike sprach die Operation Fancy Bear zu (Meyers 2016). Des Weiteren spionierten die russischen Proxy-Gruppierungen Carbanak und Gamaredon im Vorfeld des gewaltsamen Zusammenstoßes Russlands mit der Ukraine in der Straße von Kertsch 2018 ukrainische Ministerien, mit einem Schwerpunkt auf sensible Daten des Marine-Bereiches aus (Tucker 2018).

jedoch auch die 2017 gegen deutsche Energienetzwerke (attribuierter Proxy: Berserk Bear/Dragonfly) sowie die 2011 gegen US-Energienetzwerke ausgerichteten Spionage-Operationen (attribuierter Proxy: Sandworm) strategische ›Beachheads‹ für potenzielle Sabotage-Akte gegen diese Länder dar, falls sich die allgemeinen Spannungen im Zeitverlauf weiter verschärfen sollten. 2011 hatte sich das US-russische Verhältnis nach dem sog. ›Reset‹-Versuch bereits deutlich abgekühlt, nicht zuletzt aufgrund Putins Erwägungen, 2012 nach Medwedews Amtszeit erneut als Präsident kandidieren zu wollen (Tsygankov 2019, S. 41). Gleiches gilt für das deutsch-russische Verhältnis 2017, das zu diesem Zeitpunkt nicht zuletzt aufgrund der Ukraine-Sanktionen deutlich angespannt war (Manutscharjan 2017, S. 15).

Da ein direkter gewaltsamer Konflikt zwischen Russland und den USA oder Deutschland dennoch eher unwahrscheinlich erschien, wäre ein solches Vorhaben stärker der Funktion der Schwächung politischer Gegner zuzurechnen als der stärker militärisch motivierten strategischen Unterstützung im Rahmen gewaltsamer konventioneller Konflikte. Für letztere Kategorie stellt dagegen nur folgender Fall ein potenzielles Beispiel dar: 2017 veröffentlichte das kanadische Citizen Lab einen umfassenden Bericht über russische Phishing- sowie Tainted-Leaks-Operationen gegen weltweite Ziele. Darunter befanden sich auch »*senior members of the oil, gas, mining, and finance industries of the former Soviet states*«, z.B. CEOs, deren Unternehmen vor allem den Energiesektor im Kaukasus, einem Gebiet mit erheblichem ökonomischem, aber auch sicherheitspolitischem Interesse für Russland, repräsentieren (Hulcoop et al. 2017).

Eine weitere Statistik spricht ebenfalls für die Schwächung politischer Gegner im Rahmen gewaltsamer konventioneller Konflikte: So wurden zwar nur in 22 der 88 Fälle affiliierte HIIK-Konflikte erfasst, davon waren jedoch zehn gewaltsame Auseinandersetzungen. Dabei handelte es sich in erster Linie um den 2014 begonnenen Ukraine-Konflikt, jedoch wurde auch für die 2007 auf Estland ausgerichtete Cyberkampagne ein hiermit verbundener, bereits gewaltsamer HIIK-Konflikt kodiert. Gleiches gilt vor allem auch für den Georgienkrieg 2008 und die hierbei stattgefundenen, den Militäreinsatz vorbereitenden Cyberoperationen. Die durchschnittliche Intensität der Cyberoperationen im Rahmen gewaltsamer Konflikte, sei es durch Data Theft und/oder Disruption, war leicht erhöht im Vergleich zu den übrigen Proxy-Operationen (3,6 vs. 2,3), was eher für als gegen die These eskalativer Proxy-Operationen in gewaltsamen Kontexten spricht, jedoch in quantitativ geringem Maße.

Hinzu kommt, dass in vier der Fälle, in denen kritische Infrastrukturen unter den Opfern waren, ein zugrunde liegender gewaltsamer HIIK-Konflikt kodiert wurde (Power-Outage-Operation 2015 vs. Ukraine; Operation gegen ukrainisches Eisenbahnunternehmen und ukrainischen Flughafen 2015; Operation gegen ukrainischen Finanzsektor 2016; NotPetya 2017). Dies spricht zumindest partiell für die Proxy-Funktion der strategisch-operativen Unterstützung gewaltsamer konventioneller Konflikte.

Nachfolgend wird die AV I somit für die vier genannten Gruppierungen nochmal im Kontext der AV II bewertet. Dabei wird auch auf die Frage der zielspezifischen/technischen Charakteristika eingegangen, die durch den Datensatz nicht direkt abgebildet werden.

Zunächst gilt es jedoch, zwei weitere Proxy-Funktionen anhand der Daten zu diskutieren: ›Ökonomische Cyberspionage‹ sowie die ›Überwachung von Regimeeliten oder

RegimegegnerInnen im In- und Ausland‹. Für ökonomische Cyberspionage scheint es zunächst mit 16 verzeichneten Proxy-Operationen, in denen Unternehmen zum Ziel wurden, Evidenzen zu geben. Bei genauerer Betrachtung der Einzelfälle wird jedoch deutlich, dass lediglich vier bis sechs der 16 Fälle aufgrund ihres Angriffsprofils in diese Kategorie passen könnten.[68] Dass diese Fälle erst ab 2016 begonnen haben, könnte auf ein erst in den letzten Jahren entwickeltes Operationsprofil russischer Cyberproxys hinweisen. Eine alternative, plausibler erscheinende Erklärung wäre die Kontextualisierung dieser Cyberspionage-Operationen als Supply-Chain-Operationen, wie sie auch die Ende 2020 bekannt gewordene Spionage-Operation »*Solarwinds*« (gegen die gleichnamige Software-Firma und deren staatlichen sowie nichtstaatlichen Kunden) darstellte. Da in der Mehrzahl der vier bis sechs Fälle neben den Unternehmen besonders politische Institutionen/AkteurInnen unter den Zielen waren, scheint das Anvisieren der Unternehmen eher eine operativ-technische Verhaltensänderung als eine inhaltlich begründete Aufnahme der ökonomisch motivierten Cyberspionage zu sein. Ein weiteres Beispiel hierfür ist die 2018 von ESET berichtete Turla-Spionageoperation »*Mosquito*«. Für disruptive Operationen verdeutlicht dagegen die Not-Petya-Kampagne 2017 ein derartiges Vorgehen russischer Gruppierungen. Hier wurden Ziele weltweit über die Infiltration einer ukrainischen Buchhaltungssoftware infiziert, auch wenn nicht bestimmt werden kann, welche davon intendiert oder eher Kollateralschäden waren (Greenberg 2018).

Letztlich sind die Anhaltspunkte nicht ausreichend, um russischen Cyberproxys tatsächlich den funktionalen Schwerpunkt ökonomisch motivierter Cyberspionage, wie er für China deutlich aufgezeigt wurde, zu attestieren. Für einen erweiterten Untersuchungszeitraum um die Startjahre 2020 und 2021 könnte dies jedoch speziell für die Pharmaindustrie stärker der Fall sein, die nicht zuletzt im Zuge der Covid-19-Pandemie vermehrt in den Fokus staatlicher Cyberspionage-Operationen geriet (McGuire 2021).

Die Überwachung von Regimeeliten kann im Falle russischer Cyberoperationen nur über die Analyse der AV II als potenzielle Proxy-Funktion bestätigt oder kontestiert werden. Unter den erfassten Fällen ist jedenfalls keine Spionageoperation, die sich gegen inländische Regimeeliten gerichtet hätte. Im Gegensatz dazu gibt es aufseiten der AV I Hinweise für vereinzelte Spionageoperationen gegenüber RegimegegnerInnen im Ausland: Diese müssen jedoch als nichtstaatliche, zumeist zivilgesellschaftliche AkteurInnen verstanden werden. Ansonsten würde auch ein Großteil der Fälle politischer Cyberspionage in diese Kategorie fallen. Die Spionage-Kampagne »*Zebrocy*« der Fancy-Bear-Gruppierung aus 2017 zählte u.a. auch NGOs aus dem Bereich »*Family and Social Service*« zu ihren Opfern (Kaspersky 2018). Deren genaues Herkunftsland lässt sich jedoch nicht identifizieren. Im Falle der »*Monokle*«-Überwachungskampagne von 2016–2017 ließ sich

68 »*Vier bis sechs*« da teilweise nicht eindeutig war, ob die anvisierten Unternehmen tatsächlich ein Primärziel oder nicht vielmehr eine Art Nebenprodukt der eigentlich politisch-motivierten Spionageakte waren. Beispiele für die Fälle mit Unternehmen unter den Zielen, die nicht in die Kategorie der ökonomisch motivierten Cyberspionage fallen, waren u.a. die beiden Yahoo Hacks 2014 und 2015, bei denen weniger das intellektuelle Eigentum des US-Unternehmens, als deren Kundendaten ausspioniert wurden. Auch die 2007 angegriffenen estnischen Unternehmen fallen nicht in den Bereich der Cyberspionage, da sie mithilfe von DDoS-Angriffen anvisiert wurden.

dagegen feststellen, dass u.a. Personen mit Interesse am Islam, Interessierte und Anhänger der Milizgruppierung Ahrar al-Sham in Syrien sowie BewohnerInnen der Kaukasusregion ausspioniert wurden (Lookout 2019, S. 6). Aufgrund der russischen Bedrohungsperzeption gegenüber regionalen Abspaltungsaspirationen sowie terroristischen Aktionen mit islamistischer Prägung in der Konföderation scheint die Kampagne somit der Proxy-Funktion der Überwachung von RegimegegnerInnen zu entsprechen. Gleiches gilt für die Phishing-Kampagne aus 2016, die das Citizen Lab im Rahmen seines »*Tainted Leaks*«*-Reports* 2017 öffentlich machte. Hierbei waren u.a. auch »*civil society members including very high profile critics of the Russian president*« betroffen (Hulcoop et al. 2017). Auch die OSF fällt hierunter. Ihr amerikanischer Gründer George Soros ist ein vehementer Kritiker Putins und unterstützte in der Vergangenheit russische NGOs, bevor die OSF 2015 in Russland als ›unerwünscht‹ erklärt wurde (Spiegel Politik 2015).

Trotz dieser Beispiele scheint die (zumindest öffentlich bekannte) russische Spionage von RegimegegnerInnen durch Cyberproxys quantitativ nicht das Ausmaß z.B. entsprechender iranischer Cyberoperationen zu erreichen, die sich noch stärker auf DissidentInnen, Human-Rights-Organisationen, AktivistInnen sowie Personen in der Diaspora erstrecken (Zettl 2022).

Tabelle 15 fasst zusammen, für welche Cyberproxy-Funktionen auf Grundlage des HD-CY.CON hinreichende Evidenzen gefunden werden konnten. Die republikanische Ebene kann erst in Verbindung mit der Analyse der AV II im Rahmen der nachfolgenden, illustrativen Fälle bewertet werden.

Tabelle 15: Ausprägung der AV I auf Grundlage des HD-CY.CON für Russland

Starke Ausprägung	Mittlere Ausprägung	Schwache Ausprägung
Politische Cyberspionage (Beispiele: Agent.BTZ-Malware gegen das Pentagon 2008; Operation Ghost gegen europäische Außenministerien 2013–2019; Cozy-Bear-Kampagne gegen norwegische Ministerien und Parteien 2017)	Militärtechnologische Cyberspionage (Beispiele: Sandworm-Spionage-Kampagne 2009–2014; Dragonfly-Spionage-Kampagne 2011–2013).	Ökonomische Cyberspionage (kein Fall im HD-CY.CON scheint rein ökonomisch motivierte Cyberspionage gewesen zu sein)

Schwächung politischer Gegner (Staaten) ohne gewaltsamen konventionellen Konflikt (Beispiele: DDoS-Attacken gegen kirgisische Internet-Provider 2009; Leak von US-Militär-Daten 2015; DNC-Hack/Leak 2015/2016[69])	Strategisch-operative Unterstützung gewaltsamer konventioneller Konflikte (Beispiele: DDoS-Angriffe auf georgische Ziele 2008; Ukraine-Artillerie-Hack 2014)	
Schwächung politischer Gegner (Staaten) mit gewaltsamem konventionellem Konflikt (Beispiele: Estland 2007; Georgien 2008; Ukraine-Stromausfall-Hacks 2015 und 2016)	Überwachung von RegimegegnerInnen (Beispiel: Überwachungs-Kampagne Monokle 2016–2017)	
Schwächung demokratischer Institutionen/Werte (Beispiele: ClimateGate Leaks 2009; Open-Society-Foundation Tainted Leaks 2015; TV-5-Monde-Hack 2015; WADA Hack/Leak 2016)		

(Eigene Darstellung)

5.4.1.2 Die Art und Anbindung russischer Cyberproxys

Um die institutionelle Anbindung russischer Cyberproxys sowie deren generelle Akteurscharakteristika analysieren zu können, bedarf es einer qualitativen Untersuchung der für Russland maßgeblichen Proxy-Gruppierungen und ihrer Operationen. Begonnen wird mit Cozy Bear/APT29, wofür bereits 2007 der erste Vorfall im Datensatz verzeichnet wurde. Wie im Falle Chinas wird zudem die jeweilige Affiliation der Gruppierungen zu staatlichen Stellen analysiert (Tabelle 16).

Tabelle 16: Institutionelle Affiliationen der im HD-CY.CON erfassten russischen Proxys

FSB (Ziviler Inlandsgeheimdienst)	GRU (Militärgeheimdienst)	SWR (Ziviler Auslandsgeheimdienst)
Turla/Snake/Uroburos	Fancy Bear/APT28 (*Unit 26165*)	Cozy Bear/APT29
Gamaredon (*FSB-Einheit auf der Krim in Sewastopol*)	Sandworm Team/Voodoo Bear (*Unit 74455*)	

(Eigene Darstellung)

69 Democratic National Committee in den USA (DNC).

Cozy Bear/APT29

Der Gruppierung mit den geläufigsten Bezeichnungen Cozy Bear/APT29[70] wurden im Datensatz zehn Cyberoperationen zugesprochen: vier mit allgemeiner/direktstaatlicher Attribution, sechs mit staatlich gesponserter/Proxy-Attribution. Die erste Operation (allgemein/direktstaatlich) begann 2007, die zuletzt gestartete (allgemein/direktstaatlich) 2018. Alle zehn Cyberoperationen waren entweder Data Theft oder Hijacking-Operationen oder eine Kombination daraus. Cozy Bear scheint demnach weniger für öffentlichkeitswirksame, disruptive Cyberoperationsformen eingesetzt zu werden. Dies spiegelt sich auch in den Analysen von IT-Unternehmen wider, wenn sie Cozy Bear bereits seit ihren frühen Operationen ab 2007 als eine »*well-resourced, highly dedicated and organized cyberespionage group*« beschreiben (F-Secure 2015, S. 3). Wurden ihr »*fast but noisy break-in*« sowie ihre »*rapid collection and exfiltation of as much data as possible*« bemerkt (F-Secure 2015, S. 3), wechselte die Gruppierung ferner schnellstmöglich das technische Werkzeug, was ihr hohes Maß an operativer Flexibilität widerspiegelt. Dies veranschaulicht auch die eigentliche Bedeutung der Bezeichnung ›Advanced Persistent Threats‹: Darunter werden AkteurInnen verstanden, die langfristige, persistente Exfiltrationen ihrer Opfer anstreben und damit im Falle einer Detektion auch nicht zwangsläufig aufhören.

Nach der Wahl Barack Obamas 2008 spionierte Cozy Bear gezielt hochrangige MitarbeiterInnen verschiedener Ministerien sowie des Weißen Hauses aus. Begonnen hatte die Spionage-Kampagne bereits während des Wahlkampfes, entdeckt wurde sie jedoch erst 2017. Mehrjährige Spionage-Operationen sind ein zentrales Muster von Cozy Bear, wofür das beschriebene technische Sophistizierungsniveau ein zentrales Erfordernis darstellt, jedoch auch ihre Fähigkeit zu verdeckten »*intelligence gathering operations, designed to secretly penetrate a wide variety of institutions and industry*« (Stein 2017).[71] Ein Beispiel hierfür ist auch die vom IT-Unternehmen ESET als »*Operation Ghost*« bezeichnete Spionage-Kampagne: Nachdem die meisten IT-Unternehmen Cozy Bear nach dem aufsehenerregenden Hack des DNC 2016 zumindest bis November 2018 eine zeitweilige Inaktivität attestiert hatten, entdeckte ESET eine seit 2013 und bis 2019 durchweg andauernde Spionage-Kampagne, die europäische Außenministerien zum Ziel hatte (WeLiveSecurity 2019). Dies entspricht auch dem generellen Zielprofil der Gruppe, die in sieben der zehn Fälle Regierungen/Ministerien anvisierte. Aber auch (progressive) US-Think-Tanks waren zweimal unter den Opfern.

Nachfolgend werden die öffentlich bekannten Informationen über Cozy Bear als Proxy-Akteur, sowie dessen Verbindungen zu staatlichen Stellen diskutiert.

Bereits die früheste vom Datensatz erfasste Attribution durch die finnische IT-Firma F-Secure im Jahr 2015 spricht der Gruppierung ein hohes Maß an finanzieller Ausstattung sowie einen hohen Organisationsgrad zu. So schlussfolgert F-Secure für die 2007 gestartete Spionage-Operation »*Pinchduke*«: »*We therefore believe the Dukes to be a single, large, well-coordinated organization with clear separation of responsibilities and targets*« (F-

70 Weitere Namen für die Gruppierung sind zudem u.a. ›The Dukes‹ und ›Group 100‹.

71 Entsprechend dieses Spionagefokus liegt der gewichtete Durchschnittsintensität aller Cozy-Bear Operationen bei 2,1 und somit geringfügig unter dem Proxy-Gesamtdurchschnitt des Datensatzes (2,3).

Secure 2015, S. 34). Zusätzlich schließt das Unternehmen die Möglichkeit eines kriminellen Hintergrunds Cozy Bears aus und vermutet einen direkteren Nexus zu staatlichen Stellen. Im Jahr 2016 bekräftigte das US-Unternehmen CrowdStrike diese Annahmen und spezifizierte Cozy Bear als mutmaßlich mit dem zivilen Auslandsgeheimdienst SWR oder dem zivilen Inlandsgeheimdienst FSB affiliierte Proxy-Gruppierung (CrowdStrike 2020). Die US-Regierung, die bereits im Sommer 2015 durch den niederländischen Geheimdienst AIVD über die Aktivitäten Cozy Bears in Bezug auf das DNC unterrichtet wurde,[72] konzentrierte sich jedoch in ihren Anklageschriften aus 2018 ausschließlich auf die dem GRU zugeordneten Hacker und somit die noch zu behandelnde Gruppierung Fancy Bear.[73] Verantwortlich hierfür war mutmaßlich das auch beim DNC-Hack diskretere und weniger disruptive Spionage-Vorgehen Cozy Bears, das am eigentlichen DNC-Leak nicht beteiligt war.

2018 veröffentlichte der estnische Auslandsgeheimdienst einen öffentlichen Lagebericht, konkret auch zu Bedrohungen im Cyberspace durch Russland. Darin wurde Cozy Bear entsprechend der CrowdStrike-Attribution als entweder dem FSB oder dem SWR zugehörig eingestuft (Välisluureamet 2018, S. 55). Als dann im selben Jahr die niederländische Hacking-Operation bekannt wurde, erhärtete dies die SWR-Attribution. Derselbe Attributionspfad wird auch in aktuelleren Publikationen zu russischen Cybergruppierungen gewählt, z.B. des Congressional Research Service der USA (Bowen 2021). Wie die Beziehungsform zwischen Cozy Bear und dem SWR konkret ausgeformt ist, bleibt bislang – besonders in Abwesenheit einer Anklage gegen Hacker der Gruppe mit potenzieller SWR-Identifikation – noch offen. Auf diesen unklaren Hintergrund der Gruppierung verweist auch CrowdStrike in seiner aktuellsten Übersichtsdarstellung:

> »[…] it is currently unconfirmed whether Cozy Bear operations are directly performed by an internal element of SWR, or by part of an independent organization (such as a contractor or academic institution) supporting the intelligence service.« (CrowdStrike 2021a)

Somit bleibt unklar, ob es sich um ›state-ordered‹- oder ›state-integrated‹-Operationen handelt. 2017 behaupteten anonyme US-Beamte, dass der SWR mithilfe des ihm direkt verbundenen Russian Institute for Strategic Studies (RISS) ab März 2016 Pläne zur Beeinflussung der US-Wahlen auf höchster russischer Regierungsebene zirkulieren ließ. Entsprechende Dokumente lagen der berichtenden Nachrichtenagentur Reuters vor. Die darin gelisteten Maßnahmen konzentrierten sich jedoch auf Desinformationskampagnen in sozialen Medien und erwähnten in keiner Weise geplante Veröffentlichungen

72 Der AIVD hatte bereits im Sommer 2014 die Server Cozy Bears gehackt und konnte aufgrund der Sicherheitskamera-Aufnahmen am Arbeitsplatz den SWR als mutmaßlichen Auftraggeber identifizieren van Rosenthal 2018. Öffentlich bekannt wurde dies jedoch erst im Jahr 2018. Ein Jahr zuvor wurde noch ohne Nennung des AIVD bezüglich des Hacks des State Departments im November 2014 über ausländische Geheimdienstquellen berichtet, deren Informationen zur Attribution von Cozy Bear geführt hätten (Nakashima 2017).

73 Die Anklageschrift vom 13. Juli 2018 ordnete die Hacker konkret den beiden GRU Einheiten 26165 und 74455 zu. Die Einheit 26165 wird nach öffentlichem Kenntnisstand mit Fancy Bear assoziiert, die Einheit 74455 jedoch mit der im Rahmen der US-Wahlbeeinflussung seitens nichtstaatlicher Quellen keine Erwähnung findenden Hacker-Gruppierung Sandworm.

aus dem DNC-Hack (Parker et al. 2017). Dies könnte die These bekräftigen, dass Cozy Bear ab 2014 gegenüber dem DNC lediglich seine klassische politische Spionage betrieb, mit dem Leaken der Operation seitens Fancy Bear (GRU) jedoch nichts zu tun und hierüber im März 2016 auch keine Kenntnis hatte. Andererseits reflektiert dies die zentrale Rolle des SWR innerhalb der russischen Geheimdienstgemeinschaft im Rahmen politischer Spionage sowie der sog. ›aktiven Maßnahmen‹. Hinzu kommt die sich hierin ebenfalls widerspiegelnde Heterarchie russischer Geheimdienste, denen oftmals interne Konkurrenzkämpfe und fehlende Koordination auch im Cyberspace nachgesagt werden (Galeotti 2016b, S. 3–4).

Die politischen Cyberspionageoperationen von Cozy Bear entsprechen dem inhaltlichen Fokus des SWR auf politische Spionage im Ausland. Für ökonomische Spionage, die angeblich dritte Hauptrolle des SWR, lassen sich jedoch auch für Cozy Bear keine Evidenzen finden. Womöglich könnte ökonomische Spionage für Russland etwas anderes bedeuten als für China. Vorstellbar wäre die Unterstützung strategischer, geopolitischer Entscheidungen mit erheblichen Auswirkungen für die staatliche Positionierung im eurasischen Energiesektor. Es ist davon auszugehen, dass hierfür vor allem Ministerien und Botschaften in den betroffenen Ländern von russischem Interesse sein könnten, was dem Angriffsprofil Cozy Bears entspricht. Ökonomisch motivierte Cyberspionage könnte somit auch eine der Funktionen russischer Cyberproxys sein, jedoch weniger hinsichtlich eines intendierten ›Leapfroggings‹, sondern im Sinne eines von den USA als legitim erachteten Subtypus (Lotrionte 2014).

Aus operativer Sicht wird dem SWR im Cyberspace ein diskreteres, auf die Ermöglichung langfristiger Spionageoperationen ausgerichtetes Vorgehen attestiert, das mit dem beschriebenen Modus Operandi Cozy Bears korrespondiert (Bowen 2021). Ein Beispiel der jüngeren Vergangenheit ist hierfür der noch nicht vom HD-CY.CON erfasste Cyberspionage-Fall um die US-Software-Firma Solarwinds: So wurde Ende 2020 bekannt, dass tausende weltweit angesiedelte KundInnen des Unternehmens, allen voran zahlreiche US-Behörden und Institutionen, mutmaßlich durch russische Hacker kompromittiert wurden. Im April 2021 attribuierte die US-Regierung unter Joe Biden schließlich Cozy Bear und somit den SWR als mutmaßlichen Täter (Bing 2021). Dabei waren die Hacker diskret vorgegangen und schafften es, über Monate hinweg unentdeckt zu bleiben. Ihr technisches und operatives Vorgehen wurde zudem als hochgradig sophistiziert bezeichnet, im Gegensatz zum estnischen Sicherheitsbericht aus 2018, in dem der SWR diesbezüglich noch als deutlich unterhalb von FSB und GRU eingestuft worden war (Paul 2021; Välisluureamet 2018, S. 55). Diese Einschätzung steht im Widerspruch zu den Eindrücken des Privatsektors, speziell zum Bericht von F-Secure aus 2015, aber auch den aktuellsten Bewertungen von CrowdStrike (CrowdStrike 2021a). Jedoch geht aus den Berichten nicht eindeutig hervor, welche Maßstäbe hierfür angewandt wurden, die für technische Sophistizierung im Rahmen von Cyberoperationen höchst unterschiedlich ausfallen können.[74]

74 Daher ist es auch nicht verwunderlich, dass oftmals öffentlicher Dissens darüber besteht, als wie schwerwiegend und ausgefeilt eine Cyberoperation wirklich zu bezeichnen ist, mit erheblichen Implikationen für eine angestrebte Intensitätsbewertung.

Turla/Snake

Als zweite Proxy-Gruppierung mit russischem Ursprung wird nun Turla (aka Snake) behandelt.[75] Ihr wurden elf Cyberoperationen im HD-CY.CON mit nur einer allgemeinen/direktstaatlichen Attribution in einem Startzeitraum von 2008 bis 2019 zugesprochen. Wie im Falle Cozy Bears handelte es sich dabei ausschließlich um Data Theft-Kampagnen mit oder ohne Hijacking. Somit weist auch Turla einen funktionalen Schwerpunkt auf Cyberspionage auf. Fünf der elf Kampagnen dauerten mindestens zwei Jahre, was für eine gewisse Persistenz der Gruppe spricht. Dass auch bei Turla kein Doxing-Fall verzeichnet wurde, lässt wie im Falle Cozy Bears auf einen stärkeren Fokus auf verdeckt stattfindende Operationen schließen. Eine weitere Parallele zwischen den beiden Proxy-Gruppierungen stellt ihr vornehmlich politisches/staatliches Zielprofil dar, das für Turla in neun von elf Fällen vorlag. Geografisch waren in fünf Fällen Länder aus dem östlichen Teil Europas unter den betroffenen Zielen (inkl. Finnland). Hinzu kommen jedoch beispielsweise zwei Operationen, in denen (u.a.) iranische AkteurInnen betroffen waren.

Ein weiteres Charakteristikum der Gruppierung stellt ihre Spionage gegenüber Botschaften und Konsulaten, insbesondere in Staaten der früheren Sowjetunion, in vier der elf Fällen dar. Turlas durchschnittlicher Intensitätswert von 2,7 rangiert trotz des Spionage-Profils sogar noch über dem Gesamt-Proxy-Durchschnitt von 2,3, was dem noch höheren Sophistizierungsgrad und somit größeren Anteil der Hijacking-Kategorie an der Gesamtintensität der Operationen geschuldet ist.

Das technische Vorgehen der Gruppierung bezeichneten IT-Unternehmen von Anfang an als hochkomplex und anspruchsvoll. Am Anfang stand die einzige allgemein/direktstaatlich attribuierte Turla-Operation ›Agent.BTZ‹. Dabei handelte es sich um eine aufsehenerregende Spionage-Operation, die mithilfe eines USB-Sticks im Nahen Osten gestartet wurde. In der Folge wurden die vertraulichen Netzwerke des Pentagons mit der Malware Agent.BTZ infiltriert, was sowohl die Pentagon-Zentrale als auch deren Einheiten im Feld-Einsatz betraf (ThreatExpert 2008). Der Vorfall führte zu einer Gegenoperation der USA, genannt »*Operation Buckshot Yankee*«, und wurde zudem immer wieder als mitverantwortlich für die Aktivierung des US Cyber Command (US CYCOM) 2010 genannt (William J. Lynn III 2010). Erstmals als staatlich gesponserter Akteur attribuiert wurde Turla 2014 durch die deutsche IT-Firma G Data. Diese stellte in ihren technischen Berichten Verbindungen zwischen den Malwares Agent.BTZ und Uroburus sowie Turla her. Das Unternehmen konstatierte dabei wie folgt:

> »The development of a framework like Uroburos is a huge investment. The development team behind this malware obviously comprises highly skilled computer experts, as you can infer from the structure and the advanced design of the rootkit.« (G Data 2014)

Des Weiteren verfügt Turla über vielfältige Mechanismen, um Air-Gaps in Zielsystemen zu überwinden (Tanase 2015). Der physische Hardware-Infektionsweg über eine Person, sei es ein Agent oder ein umgedrehter Insider, wie er im Falle des Pentagon-Hacks angewandt wurde, stellt nur ein Beispiel dar. Hinzu kommt ein hohes Maß an aspirierter

75 Weitere Namen aus der IT-Wirtschaft sind u.a. ›Venomous Bear‹ und ›Waterbug‹.

›Operational Security‹ der Gruppierung, um die Detektion sowie Vereitelung der eigenen Operationen zu verhindern. Gleiches gilt auch für Handlungen zur Verschärfung des Attributionsproblems. Im Falle Turlas handelt es sich hierbei etwa um die Nutzung distinkter Command-and-Control-Netzwerke, ermöglicht durch begleitende SIGINT-Operationen (CrowdStrike 2021b).

Ein weiterer Fall der Turla-Gruppe, der besondere Aufmerksamkeit erfahren hat, war der Hack des Schweizer Verteidigungsunternehmens RUAG von 2014–2016. Während das Schweizer Cybersicherheits-Zentrum in seinem zum damaligen Zeitpunkt für staatliche Behörden eher ungewöhnlich technisch detaillierten Bericht lediglich die mit Turla assoziierte Malware erwähnte, wurde darauf aufbauend schnell der Link zur Spionage-Gruppe Turla und somit Russland hergestellt (Kovacs 2016). Die Operation bekräftigt zudem die russische Cyberproxy-Funktion der militärtechnologischen Spionage.

Mithilfe von False-Flag-Attacken können AngreiferInnen im Cyberspace ihre Identität verschleiern und den Verdacht auf einen anderen Akteur lenken. Die wohl bekannteste Anwendung dieser Strategie attestierte im Juni 2019 das US-Unternehmen Symantec der Turla-Gruppierung. Zuvor hatten die IT-Forscher herausgefunden, dass Turla in zumindest einem Spionage-Fall gegenüber einem Ziel im Nahen Osten die Angriffsinfrastruktur der iranischen Proxy-Gruppe OilRig/APT34/Crambus gekapert und somit den Verdacht auf diese gelenkt hatte. Britische und amerikanische Regierungsbeamte bestätigten dieses Vorgehen im Oktober 2019 für weitere Ziele. So hatte Turla nicht nur die Command-and-Control-Server von OilRig benutzt, sondern auch Zugriff auf deren Spionage-Ziele sowie den für den Nachbau iranischer Malware-Tools notwendigen Code erlangt (Stubbs und Bing 2019). Primäres Ziel von Turla war hierbei offensichtlich, unerkannt zu bleiben.

Auf institutioneller Ebene wird Turla dem inländischen Geheimdienst FSB zugeordnet. Sowohl tschechische als auch estnische Behörden attribuierten das direkte Nachfolgesubjekt des sowjetischen KGB als für Turla hauptverantwortliches Staatsorgan (Hovet 2018). Zentrale Aufgaben des FSB sind im Rahmen der russischen Geheimdienstarchitektur »*political security*« und »*counter intelligence*« (Galeotti 2016b, S. 3). Seinen per Definition domestischen Fokus weitete der FSB jedoch im Laufe der Jahre sukzessive aus, auf analoger Ebene im Rahmen von »*extrajudicial killings*« (Walton 2018).[76] Zwar wurden keine Cyberoperationen Turlas gegenüber inländischen Zielen registriert, jedoch verfügt der FSB seit 1995 über die autoritative Hoheit des sog. ›System of Operational-Investigatory Measures‹ (SORM). Dieses verpflichtet russische Telekommunikationsanbieter dazu, Überwachungshardware des FSB in ihre Produkte einzubauen, wodurch Spionage domestischer RegimegegnerInnen, jedoch auch von Regimeeliten auf nationaler Rechtsgrundlage ermöglicht wird (Maréchal 2017, S. 33).

Ob es sich bei Turla um einen direkten FSB-Ableger oder um eine unabhängigere Hacking-for-Hire-Gruppierung handelt, ist (öffentlich) bislang nicht eindeutig geklärt. Fest steht, dass Turla über massive finanzielle und organisatorische Ressourcen zu verfügen scheint, was jedoch auch für ein hohes Maß an staatlicher Unterstützung (›state-

76 Ein prominentes Beispiel hierfür war die dem FSB angelastete Ermordung des russischen Ex-Agenten Alexander Litwinenko 2006 im Londoner Exil.

ordered‹) und nicht zwingend für direktstaatliche Akteurschaft sprechen kann. Grundlegend bewies der FSB in weiteren Cyberoperationen, z.B. den Yahoo-Hacks, eine Affinität zur Instrumentalisierung inländischer oder ausländischer HackerInnen. So arbeiteten laut einer US-Anklage aus 2017 zwei FSB-Agenten direkt mit zwei Cyberkriminellen, Alexsey Belan und Karim Baratov, bei den Hacks der mindestens 500 Millionen Yahoo-Accounts zusammen. Die Agenten hätten Letztere dabei »*protected, directed, facilitated and paid*« (DoJ 2017), was auf eine physische, inhaltliche sowie finanzielle Unterstützung der Proxys hinweist (mindestens ›state-coordinated‹). Bei Alexsey Belan handelte es sich seit 2013 um einen der »*FBI's Cyber Most Wanted Criminals*«. Nachdem er auf internationalen Strafbefehl hin in Europa gefasst wurde, entkam er aus der Haft und floh nach Russland. Anstatt Belan an die USA auszuliefern, nutzten die beiden FSB-Agenten seine Fähigkeiten, um die Yahoo-Hacks zu ermöglichen. Sie statteten Belan mit umfassenden Strafverfolgungs- und Geheimdienstinformationen aus, die ihm halfen, einer Detektion durch die USA zu entgehen. Dies beinhaltete u.a. FSB-interne Werkzeuge zur Überführung von Cyberkriminellen (Indikatoren für ›state-ordered‹). Zusätzlich gestatteten sie Belan, seine Infiltrationen der Yahoo-Accounts auch zur persönlichen Bereicherung in Form von Kreditkarteninformations-Diebstahl zu nutzen. Zuletzt ist ein weiteres Detail der Anklageschrift relevant: So heißt es in der Zusammenfassung, unter den von Belan gehackten Accounts seien einige von besonderem Interesse für den FSB gewesen:

> »[...] a foreign intelligence and law enforcement service, such as personal accounts belonging to Russian journalists; Russian and U.S. government officials; employees of a prominent Russian cybersecurity company; and numerous employees of other providers whose networks the conspirators sought to exploit.« (DoJ 2017)

›Russische Regierungsbeamte‹ deuten auf die Proxy-Funktion der Überwachung von Regimeeliten hin, die primär auf der republikanischen Ebene des Liberalismus verortet wurde. Die Infiltration der Accounts russischer JournalistInnen kann dagegen als ein weiterer Fall der Überwachung von RegimegegnerInnen, diesmal im Inland, gewertet werden. Die beiden Yahoo-Hacks stützen somit die bereits aus dem konventionellen Bereich für den FSB berichtete Nutzung von Kriminellen als Proxys (Satter 2003; Galeotti 2017). Im Falle des nach Russland geflohenen Belan ist von einer primär auf Zwang basierenden Beziehungsform zwischen FSB und Proxy auszugehen: Sofern er nicht in die USA ausgeliefert werden wollte, musste sich Belan in die Rolle des Cyberproxys begeben. Gleichzeitig zeugt das hohe Maß an zur Verfügung gestellten Geheimdienstinformationen entweder von einem großen Vertrauen der Agenten in ihre eigenen Proxy-Überwachungsfähigkeiten oder von einem zusätzlich ideell-patriotischen Element aufseiten Belans, der seine Ermächtigung nicht gegen den FSB selbst richten würde.

Da Turla als eine Art institutionalisierter FSB-Proxy mit einem mehrjährigen Aktionszeitraum angesehen wird, scheint die ad-hoc-Instrumentalisierung von Cyberkriminellen dem FSB für solch besonders brisante Spionagefälle dienlich zu sein, z.B., wenn nicht nur ausländische Regierungen oder Botschaften, sondern auch russische Regierungsangehörige unter den Zielen sind. Sofern für Turla weniger von einer Zwangs- als einer freiwilligen Proxy-Rollenübernahme ausgegangen werden kann, könnte für die Gruppierung auch die effektive Kontrolle des FSB eingeschränkter sein als für Cyberkriminelle wie Belan. Eine eingeschränkte Proxy-Kontrolle ist für Cyberspionage

gegenüber externen Rivalen ein prinzipiell geringeres Problem. Die Überwachung von domestischen Regierungsmitgliedern könnte dagegen patriotische Ressentiments aufseiten der Hacker hervorrufen oder sie dazu verleiten, ihr Wissen an besagte Personen zu verkaufen und somit die Kampagne zu vereiteln.

Im Falle des Yahoo-Hacks sind jedoch nicht nur die angeklagten Proxys von Interesse, auch einer der beiden FSB-Agenten sollte genauer betrachtet werden. Dmitri Dokuchaev führte bereits während seiner Zeit beim Geheimdienst eine parallele Karriere als Cyberkrimineller. Anfang 2017 wurde er schließlich zusammen mit einem ihm überstellten hochrangigen Beamten sowie einem Mitarbeiter der IT-Firma Kaspersky in Russland wegen Verrats und der Weitergabe geheimer Informationen an die USA angeklagt und verurteilt. Hierbei soll es sich laut Medienberichten um Ermittlungsdaten bezüglich des Cyberkriminellen Wladimir Fomenko gehandelt haben, über dessen Server mutmaßlich APT28/Fancy Bear und somit der GRU seine Cyberoperationen gegen Wahlinfrastruktur in den USA (u.a. Illinois und Arizona) 2016 durchführte (O'Neill 2017; Calabresi 2017). Die Episode könnte somit ein Beispiel für russische Behördenkämpfe gewesen sein, worin der FSB einem ausländischen Geheimdienst Informationen über die Cyberoperationen des GRU geliefert haben könnte und hierfür in der Folge auf angebliche Initiative des GRU hin vor Gericht gestellt wurde (The Bell 2017).

Zuvor beschuldigten Cyberkriminelle den hochrangigen FSB-Oberst Sergei Michailow, über den US-Hack-Fall hinaus gegen Bezahlung jahrelang Informationen über Cyberkriminelle an westliche Geheimdienste weitergegeben zu haben (Krebs 2017).[77] Inwiefern diese Behauptungen der Wahrheit entsprechen oder mehr das Resultat eines persönlichen Rachefeldzugs sind, kann an dieser Stelle schwer beurteilt werden. Nichtsdestotrotz verdeutlichen alle aufgezählten Entwicklungen im Rahmen des Yahoo-Hacks und der daran beteiligten Personen, dass fluide Verbindungen zwischen russischen Geheimdiensten, Cyberkriminellen und anscheinend auch Unternehmen wie Kaspersky existieren, die auf informell-persönlichen Beziehungen, jedoch ohne tiefergehende Loyalitäten beruhen. Das persönliche Eigeninteresse, im russischen Sicherheitsapparat und dessen erweiterter Einflusssphäre über die Zeit bestehen zu können, fungiert als Hauptmaxime der AkteurInnen. Zusammengefasst verdeutlichen die Yahoo-Hacks, dass der russische FSB seiner Rolle zur Wahrung der ›Political Security‹ im Cyberspace allem Anschein nach u.a. mithilfe einzelner Cyberkrimineller nachkommt. Zwar befinden sich diese in faktischer Abhängigkeit vom russischen Staat, können sich jedoch auch gegen AkteurInnen des Sicherheitsapparates wenden.

Ein weiteres Beispiel für das dem FSB zugeordnete Beziehungsgeflecht zu Cyberkriminellen stellen die Sanktionen des US-Finanzministeriums gegen die Mitglieder der Gruppe ›Evil Corp‹ aus 2019 dar. Diese hatten weltweit Malware gegen Finanzinstitute und Banken eingesetzt, um deren Login-Daten zu erbeuten. Daraus ging ein erheblicher finanzieller Schaden für die Betroffenen hervor (DoT 2019). Im Zuge der Sanktionen brachte das Finanzministerium den Anführer von Evil Corp, Maksim Yakubets, direkt mit dem FSB in Verbindung. Ab dem Jahr 2017 habe er für den Geheimdienst gearbeitet u.a. »*on projects for the Russian state, to include acquiring confidential documents through*

77 Den Kriminellen war vorher angeblich Straferlass im Gegenzug für Hacking-Dienstleistungen angeboten worden.

cyber-enabled means and conducting cyber-enabled operations on its behalf « (DoT 2019). Genau genommen wird aus der Stellungnahme des Ministeriums jedoch nicht ersichtlich, ob auch besagte Kriminalitätsmalware auf Geheiß des FSB durch Evil Corp eingesetzt wurde. Theoretisch könnte es sich bei der Gruppe auch um Moonlighter handeln.

Für die weitere Analyse ist zudem wichtig, dass dem FSB besonders enge Beziehungen zu Wladimir Putin nachgesagt werden, der dem Geheimdienst zeitweilig vorstand und auch schon dem KGB angehörte (Dawisha 2015; Marten 2017). Hinzu kommen die erwähnten Revierstreitigkeiten der unterschiedlichen Geheimdienste, allen voran zwischen den zivilen Diensten FSB/SWR und dem militärischen GRU.

Fancy Bear/APT28/Sofacy[78]

Als dritte Proxy-Gruppierung Russlands wird Fancy Bear/APT28 vorgestellt. Mit 33 attribuierten Cyberoperationen ist die Gruppierung am häufigsten im HD-CY.CON vertreten. 15 Fälle wurden als allgemeine/direktstaatliche und 18 Operationen als staatlich gesponserte Proxy-Attribution kodiert. Beginnend im Jahr 2007 unternahm die Gruppierung zunächst umfangreiche Spearphishing-Kampagnen, vor allem gegenüber osteuropäischen Zielen wie Regierungen, Ministerien, staatlichen Behörden, aber auch JournalistInnen. Ab 2011 wurden auch gezielt georgische Institutionen, etwa das Außenministerium, anvisiert (FireEye 2014). Hinzu kamen im weiteren Verlauf bis 2014 Ziele der NATO sowie TeilnehmerInnen europäischer Rüstungsmessen.

28 der 33 erfassten Fancy-Bear-Operationen waren Data Theft/Hijacking-Vorfälle in einem Zeitraum von 2014 bis 2019 (Startjahre). Sieben davon waren jedoch keine reinen Spionage-Operationen, sondern Hack-and-Leak-Vorfälle (Doxing).[79] Dieses ab 2015 regelmäßig angewandte Vorgehen stellt ein zentrales Charakteristikum der Gruppe dar.[80] Doxing-Operationen zielen wesentlich öffentlichkeitswirksamer auf die Schwächung politischer GegnerInnen, aber auch demokratischer Institutionen im Allgemeinen ab, als Cyberspionage-Operationen, die nicht zwingend öffentlich werden müssen. Das Bekanntwerden eines Datendiebstahls kann die Reputation des Opfers zwar ebenfalls schwächen, jedoch nicht auf inhaltlicher Ebene, sondern ausschließlich im Sinne einer nicht ausreichenden IT-Verteidigungsstrategie. Der Diebstahl und das Veröffentlichen sensibler bzw. kompromittierender Daten unterminieren einen politischen Kontrahenten jedoch konkret auf ideeller Ebene, etwa wenn Verfehlungen demokratischer Regierungen oder Institutionen bekannt werden, die den Grundprinzipien demokratischen Regierens entgegenstehen. Besondere Brisanz erfahren solche Leaks im Vorfeld politischer Wahlen. Bekanntestes Beispiel hierfür waren die Fancy Bear-Operationen im Rahmen des US-Wahlkampfes 2016. Weitere Doxing-Operationen der Fancy Bear-Gruppierung waren der WADA-Leak aus 2016, das Doxing von Informationen der Brad-

78 Weitere Namen (u.a.): ›Pawn Storm‹ und ›Tsar Team‹.

79 In einem weiteren Fall kam es zu Data Theft + Doxing und Disruption (Tainted Leaks gegen OSF 2015).

80 Im Zeitraum von 2017–2019 verzeichnet der HD-CY.CON fünfzehn weitere gestartete Fancy-Bear-Spionageoperationen (Data Theft mit/ohne Hijacking). Die bis 2014 im Fokus stehende, ›reine‹ Cyberspionage wurde somit auch in der Folge fortgesetzt.

ley-Foundation 2016 sowie das Veröffentlichen kompromittierender E-Mail-Inhalte des deutschen UN-Botschafters im Jahr 2017.[81]

Neben diesen auf informationeller Ebene ›disruptiven‹ Doxing-Operationen wurden Fancy Bear lediglich in vier Fällen auch stärker technische Störungen zugewiesen. 2015 hackte die Gruppe den französischen TV-Sender TV5 Le Monde, unterband zeitweilig die komplette Übertragung des Senders, übernahm dessen Facebook- und Twitter-Accounts und postete islamistische Propaganda. Somit sollte der Anschein einer religiös-fundamentalistischen Cyber-Attacke einer Gruppierung mit dem Namen ›Cyber Caliphate‹ erweckt werden. Untersuchungen entlarvten die Operation jedoch als False-Flag-Attacke und Fancy Bear/APT28 als eigentlichen Ursprung. Interessant ist eine operativ-taktische Gemeinsamkeit zum ebenfalls 2015 erfolgten Stromausfall in der Ukraine: So waren auch im Falle des TV5-Monde-Hacks begleitende Störungen der internen Kommunikationsmöglichkeiten des Opfers geplant, um dessen Reaktionsoptionen einzuschränken (Schwartz 2017).[82]

Mit einer durchschnittlichen Intensität von 2,2 rangiert Fancy Bear leicht vor Cozy Bear (2,1), jedoch hinter Turla mit 2,7. Da Data Theft in seiner Intensität durch die Zusatzkodierung von Doxing im HD-CY.CON nicht steigt, führten die zahlreichen Hack-and-Leak-Operationen Fancy Bears auch nicht zu einer noch stärker erhöhten Intensität in Abwesenheit sonstiger Operationsformen mit disruptiver Auswirkung. Des Weiteren waren 14 Fancy-Bear-Operationen ausschließliche Data Theft-Fälle ohne Hijacking.

Den operativ weniger auf physische Sabotage und mehr auf den Gewinn und die strategische Verwendung sensibler Informationen ausgerichteten Fokus der Gruppe belegt auch das erwähnte Beispiel der Spionage-Operation gegen ukrainische Militär-Streitkräfte mithilfe einer infizierten App 2015. Zwar kann dieser Vorfall als einziger einem gewaltsamen konventionellen Konflikt zugeordnet werden, hatte hierbei jedoch keine physischen Schäden zum Ziel. Vier weitere Fancy-Bear-Spionage-Operationen weisen einen kodierten Konflikt des HIIK-Barometers auf. Diese waren jedoch alle gewaltlos und bezogen sich auf ideologisch-systemische ›International-Power‹-Konflikte mit den USA (drei Fälle) und Deutschland (ein Fall).

Bereits 2014 hatte das US-Unternehmen FireEye Fancy Bear als mutmaßlich russischen Proxy bezeichnet: »*While we don't have pictures of a building, personas to reveal, or a government agency to name, what we do have is evidence of long-standing, focused operations that indicate a government sponsor – specifically, a government based in Moscow*« (FireEye 2014). Der jedoch bislang zentrale Attributionsschub fand im Anschluss an die US-Wahlen 2016 statt:

81 Die geleakten Mails legten offen, dass Christoph Heusgen seiner Frau einen Job bei der UN besorgt habe, was aus russischer Sicht die Korruption westlicher Eliten demonstrieren würde (Mischke 2017).

82 Im Falle des VPN-Filter Botnetzes wurden innerhalb der IT-Community ebenfalls Befürchtungen laut, Fancy Bear könne die erlangte Kontrolle über ein Netz aus weltweit über 500.000 gekaperten Routern, mit überwiegendem Anteil in der Ukraine, für disruptive Cyberangriffe auf Ziele des Landes nutzen. Im Mai 2018 erhielt das FBI seitens eines US-Gerichts die Erlaubnis, die für die Kontrolle des Botnetzes verantwortliche Internet-Domain zu beschlagnahmen, um somit mögliche Sabotage-Akte, jedoch auch weitere, weltweit angelegte Cyberspionage zu unterbinden (Finkle und Polityuk 2018).

Im Juni hatte CrowdStrike auf seiner Webseite eine Attribution des DNC-Hacks in Richtung Cozy Bear und Fancy Bear veröffentlicht und dabei erstmals eine Verbindung zwischen Fancy Bear und dem GRU hergestellt:

> »Extensive targeting of defense ministries and other military victims has been observed, the profile of which closely mirrors the strategic interests of the Russian government, and may indicate affiliation with Главное Разведывательное Управление (Main Intelligence Department) or GRU, Russia's premier military intelligence service.« (CrowdStrike 2016)

In seinem Hintergrundbericht zur russischen Wahlbeeinflussung vom 6. Januar 2017 konstatierte das Office of the Director of National Intelligence (ODNI) zwar, dass es den GRU als verantwortlichen Akteur für die Hack-and-Leak-Operationen hielt, erwähnte jedoch weder Fancy Bear, Cozy Bear noch den SWR (ODNI 2017). Dies änderte sich auch nicht mit den sog. ›Mueller-Indictments‹ vom Juli 2018: Zwar wurden hier explizite Teilaufgaben innerhalb des DNC-Hacks/Leaks einzelnen angeklagten GRU-Mitgliedern angelastet. Diese wurden zudem entweder der GRU-Einheit 26165 oder 74455 zugeordnet. Jedoch lässt sich auch in Verbindung mit den Berichten privater IT-Firmen nur schwer herausfinden, ob Fancy Bear tatsächlich aus Mitgliedern beider GRU-Einheiten besteht oder nur der Einheit 26165, wie es seitens der Medien im Nachgang der Anklage kolportiert wurde und auch im Rahmen dieser Arbeit als das plausiblere Szenario angesehen wird (Graff 2018). Die in der Anklageschrift erwähnten Mitglieder der GRU-Einheit 74455 haben Fancy Bear wahrscheinlich lediglich unterstützt, ohne der Gruppierung dauerhaft anzugehören. Eine Möglichkeit wäre, dass sie Teil einer anderen zeitweilig mit Fancy Bear kooperierenden russischen Cyberproxy-Gruppierung sein könnten. Auch die Anklage gegen weitere GRU-Beamte aus 2020 verschafft keine Klarheit: Hier wurden Agenten der Einheit 74455 als Mitglieder des im Anschluss zu behandelnden zweiten GRU-Proxys Sandworm identifiziert. Da unter den angeklagten Personen jedoch keine der 2018 genannten 74455-Agenten zu finden waren, bleibt deren genauere Affiliation weiterhin unklar. Es ist jedoch davon auszugehen, dass die Einheit 74455 nicht nur aus AkteurInnen des Sandworm-Kollektivs besteht.[83]

Auch wenn besonders dem FSB eine stetige Ad-hoc-Kooperation mit Kriminellen im konventionellen sowie Cyberraum unterstellt wird, gibt es auch für den GRU-Ableger Fancy Bear Hinweise hierauf: Die Hacktivisten-Gruppierung CyberBerkut wird in der Ukraine verortet und verfolgt mit ihren DDoS-Angriffen und sonstigen Cyberoperationen Ziele der russischen Separatisten in der Donbass-Region. Eine finnische IT-Firma beschreibt den Hintergrund CyberBerkuts folgendermaßen: »*It's a voluntary cyber offensive unit that's not closely affiliated with any government*« (Stone 2015b). Auch Tim Maurer bezeichnet CyberBerkut als Beispiel eines indirekten Proxys, der allenfalls ideologische Unterstützung/Anreize erhalte (›state-encouraged‹). Der Ursprung der Gruppe wird in russischen Cyberkriminellen-Foren vermutet (Stone 2015b).

Die nachfolgende Beschreibung der Beziehung zwischen dem russischem Staat und CyberBerkut durch CrowdStrike 2015 kann dagegen nicht eindeutig klären, ob es

83 Interview mit einem Beamten einer deutschen Bundesbehörde im IT-Bereich, 20. April 2021.

sich um ›state-encouraged/state-shaped‹ oder doch bereits ›state-coordinated/state-ordered‹ Operationen der Gruppierung handelt(e):

> »There are indications that CyberBerkut has ties to Russian state security. These indications are based on several factors. First, CrowdStrike has identified specific correlations between the group's interference in Ukrainian national elections and the messaging delivered by Russia-owned state media that signify close coordination. Additionally, there are significant parallels between the current techniques employed by CyberBerkut and those used in previous conflicts associated with Russia, namely the conflict in Estonia in 2007.« (CrowdStrike, S. 29)

Ein Jahr später wurde jedoch der bereits 2015 erwähnte Link zwischen CyberBerkut und Fancy Bear weiter untermauert, ein Indiz für eine zumindest zeitweilig direktere Verantwortlichkeit des Staates. Im Rahmen seiner Untersuchung der Hacking-Operationen gegen das Investigativ-Journalismus-Kollektiv Bellingcat, das u.a. den Absturz der malaysischen MH17-Maschine über der Ukraine untersucht und Beweise für eine russische Verantwortlichkeit veröffentlicht hatte, plausibilisierte das US-Unternehmen ThreatConnect eine Zusammenarbeit zwischen CyberBerkut und Fancy Bear (ThreatConnect 2016). Da der GRU umfassend im Ukrainekonflikt aktiv ist, erscheint eine solche Zusammenarbeit zwischen einer prorussischen Hacker-Gruppierung sowie einem direkteren russischen Cyberproxy durchaus denkbar. Gestützt wird diese These auch durch die stärker informationsgetriebenen Cyberoperationen, die Fancy Bear im Gegensatz zu Sandworm ebenfalls mit CyberBerkut gemeinsam hat.

Hinsichtlich des technischen Vorgehens Fancy Bears erscheinen deren oftmals relativ einfach gehaltenen Angriffsstrukturen bemerkenswert, werden dem GRU doch im Vergleich der russischen Geheimdienste die technisch umfangreichsten Fähigkeiten attestiert (Välisluureamet 2018, S. 55). Ein Grund hierfür könnte sein, dass für die intendierten Funktionen Fancy Bears das Kreieren maßgeschneiderter Malware nicht notwendig ist, sondern z.B. über Spearphishing-Operationen die besten Chancen einer Ziel-Infiltration bestehen. Zusätzlich können grundlegend simple Angriffsmethoden, wie sie Fancy Bear 2020 bescheinigt wurden (Hacquebord und Remorin 2020), eine Attribution erschweren und fälschlicherweise auf einen weniger versierten Akteur hindeuten (Steffens in Tanriverdi 2018).[84]

Sandworm/Black Energy/Vodoo Bear[85]

Als vierte Cyberproxy-Gruppierung Russlands steht nun Sandworm im Fokus. Von 2009 bis 2019 (Startjahre) wurden ihr 13 Cyberoperationen im HD-CY.CON zugesprochen. Davon wurden sechs Fälle als staatlich gesponserte sowie sieben als allgemeine/direktstaatliche Attributionen kodiert. Hinsichtlich der erfassten Incident-Types weicht Sandworm von der für Cozy Bear und Turla prävalenten Cyberspionage maßgeblich ab: In lediglich vier von 13 Fällen waren Data Theft und/oder (in Kombination) mit Hijacking das Mittel der Wahl. In einem zusätzlichen Fall kamen alle drei Incident-Types zur Anwendung.

84 Nichtsdestotrotz besitzt Fancy Bear die Fähigkeiten, eigene Malware zu entwickeln, wie im Falle der Spionage-Software X-Agent Meyers 2016.

85 Weitere Bezeichnungen: ›Telebots‹ und ›Iron Viking‹.

Somit waren die übrigen neun Cyberoperationen ausschließlich disruptiver Natur. Die durchschnittliche Intensität aller Operationen Sandworms im Datensatz erreicht einen im Vergleich zu Cozy Bear, Turla und Fancy Bear deutlich erhöhten Wert von 3,8, dies bestätigt sich ebenfalls bezüglich der Durchschnittsintensität aller im Datensatz verzeichneten Proxy-Operationen (2,3). Sandworm weist somit ein funktional distinktes Operations-Profil auf: So wird die auch für diesen Proxy vorzufindende Cyberspionage durch disruptivere Operationsformen mit teilweise sogar physischen Effekten komplettiert.

Die Ende 2015 und 2016 in der Ukraine verursachten Stromausfälle wurden jeweils Sandworm mithilfe der BlackEnergy-Malware zur Erlangung umfangreicher Zugriffsrechte sowie der Malware Kill Disk zur letztlichen Ausführung der Systemstörung angelastet (Thomas Colatin 2019). Cybersabotage-Akte gegen die Steuerungssysteme kritischer Infrastrukturen (SCADA) blieben bislang auch nach Stuxnet ein kaum verzeichnetes Phänomen; somit sind diese beiden Cyberangriffe wichtig für die funktionale Analyse von Sandworm. Beide Angriffe erfolgten im Rahmen des gewaltsamen Ukraine-Konfliktes, was die Schwächung politischer Gegner während bewaffneter Konflikte als angestrebte Funktion bekräftigt. Im Gegensatz zu den vorbereitenden Cyberoperationen in unmittelbarer zeitlicher Nähe zu konventionellen Militärschlägen 2008 in Georgien waren mit den Stromausfällen keine unmittelbaren taktischen Zugewinne auf dem analogen Schlachtfeld verbunden. Zwei Intentionen wurden hierfür stattdessen besonders häufig debattiert. Erstens das Signalisieren der eigenen Kapazitäten gegenüber dem militärischen Kontrahenten und dessen Bevölkerung, auch im Sinne eines ›Attrition‹-Zuges, letztlich zur Unterminierung/Schwächung der Gegenpartei (Pernik 2018). Zweitens das Testen solch komplexer Angriffssysteme im Rahmen eines auf der allgemeinen Ebene bereits eskalierten Konfliktes, indem mögliche Kollateralschäden oder Eskalationspotenziale eine deutlich untergeordnete Rolle spielen als im Falle eines ähnlichen Cyberangriffes ohne zugrunde liegendem, gewaltsamem Konflikt (Zetter 2017a; Cerulus 2019).

In drei der Sandworm-Operationen handelte es sich um Data Theft und/oder Hijacking-Operationen gegen kritische Infrastrukturen. In Kombination mit den verzeichneten Sabotage-Akten gegenüber kritischen Infrastrukturen im Rahmen militärischer Auseinandersetzungen unterstreicht dies zusätzlich den wesentlich stärker disruptiv-offensiven Charakter der Aktionen Sandworms, wird dies als Spionage zur Vorbereitung künftiger Angriffe gewertet. Hiervon war besonders die Ukraine betroffen, da das Land in neun Fällen das alleinige Zielland darstellte. Zudem führte Sandworm insbesondere auch gegenüber den USA öffentlichen Berichten zufolge bereits ab 2011 Aufklärungsmissionen gegenüber kritischen Infrastrukturen durch (Cloherty und Thomas 2014).

Neben den beiden Stromausfällen am meisten Aufsehen erregt haben jedoch die Wiper-/Ransomware-Kampagne ›NotPetya‹ 2017 sowie die Malware-Kampagne ›Olympic Destroyer‹ gegen die olympischen Winterspiele 2018 in Südkorea. In beiden Fällen störte Sandworm die Zielsysteme durch Wiper-Angriffe in ihrer Funktionalität, was somit nichts mit Cyberspionage zu tun hatte, auch wenn für Olympic Destroyer aufgrund des Diebstahls von Zugangsdaten ebenfalls Data Theft kodiert wurde, was letztlich jedoch ebenfalls der Sabotage diente. Im Falle von NotPetya kommt hinzu, dass die Angreifer die weltweit erfolgten Schäden anscheinend billigend in Kauf nahmen, musste doch nach der ursprünglichen Infiltration einer ukrainischen Buchhaltungssoftware damit gerechnet werden, dass die Malware nicht nur auf die anfänglich anvisierte Ukraine würde be-

schränkt bleiben (Greenberg 2018). Die Folge waren finanzielle Verluste in Milliardenhöhe, besonders das dänische Unternehmen Maersk entkam nur knapp einem noch disruptiveren Szenario: So konnte das Unternehmen nur durch Zufall auf ein nicht NotPetya zum Opfer gefallenes Backup der eigenen Netzwerkinfrastruktur (Domain-Controller) eines Unternehmensstandorts in Ghana zurückgreifen, da dieses während der Kampagne aufgrund eines Stromausfalls nicht am Netz angeschlossen war (Greenberg 2019b, S. 194). Bei Olympic Destroyer ist bemerkenswert, dass Sandworm den Anschein einer nordkoreanischen Operation erwecken wollte, was auf eine zusätzlich intendierte Disruptions-Funktion der False-Flag-Attacke auf geopolitischer Ebene schließen lässt (Marks 2019).

Im Verlauf des Jahres 2017 brachte die IT-Community eine weitere Malware mit Sandworm in Verbindung: So wurden Ähnlichkeiten zwischen der Ransomware ›BadRabbit‹ und BlackEnergy festgestellt. Da die disruptive Verwendung der BlackEnergy3-Version ausschließlich Sandworm attestiert wurde, kann hier ein Attributionslink hergestellt werden.[86] BadRabbit unterschied sich jedoch auch von NotPetya/BlackEnergy: So war BadRabbit keine Wiper-Malware, sondern eine tatsächliche Ransomware. Zusätzlich nutzte BadRabbit gleich drei verschiedene Open-Source-Tools im Rahmen seiner Angriffsinfrastruktur (Mimikatz, DiskCryptor und ReactOS; Johnson 2017). Bemerkenswert ist zudem die geografische Verteilung der Opfer: Laut IT-Unternehmen Avast waren 71 Prozent hiervon russisch, gefolgt von ukrainischen Zielen mit 14 Prozent. Konkrete Ziele waren u.a. das»Ministry of Infrastructure of Ukraine, Odessa's airpor t, Kiev's subway and two Russian media groups« (Zezula et al. 2017). Infiziert wurden die Opfer über Watering-Hole-Operationen gegenüber russischen News-Webseiten wie Interfax. Die üblicherweise auf finanziellen Gewinn ausgerichteten Ransomware-Angriffe fügen sich weniger plausibel in das sonstige Operationsschema von Sandworm ein. Es kann jedoch auch das bloße Stören der operativen Geschäfte der überwiegend dem kommerziellen Sektor angehörenden Opfer das Primärziel gewesen sein. Womöglich waren auch die erwähnten ukrainischen Opfer die eigentlichen Primärziele und alle weiteren Infizierungen entweder ein positiver finanzieller Nebeneffekt oder ein in Kauf genommener Kollateralschaden, ähnlich wie bei der NotPetya-Kampagne, bei der letztlich auch das russische Staatsunternehmen Rosneft betroffen war.

2018 lastete das britische National Cyber Security Centre (NCSC) mit ›High Confidence‹ dem russischen GRU die BadRabbit-Kampagne an. Aus der Bekanntmachung ging jedoch nicht explizit hervor, ob hierfür eher Sandworm oder Fancy Bear als dominierende GRU-Cyberakteure verantwortlich gemacht werden (NCSC 2018b). Entsprechend dem disruptiveren Vorgehen Sandworms sowie dem technischen Nexus zwischen BadRabbit und NotPetya erscheint die Sandworm-Attribution jedoch plausibler.

Das technisch-taktische Vorgehen Sandworms wird als komplex und sophistiziert beschrieben. Als Einstiegstor für den ersten Stromausfall in der Ukraine 2015 dienten bereits ein halbes Jahr zuvor durchgeführte Phishing-Operationen. Die eigentliche Cyberoperation beinhaltete zusätzlich flankierende DDoS-Attacken zur Unterstützung des Sabotage-Aktes:

86 Der ukrainische Geheimdienst attribuierte 2017 jedoch Fancy Bear als für BadRabbit verantwortlich (Bing 2017b).

> »In addition to opening breakers at substations, the Sandworm Team explored methods to extend the blackouts. They carried out a denial of service attack against one company's call center, flooding it with fake calls to stop company personnel from identifying the blackout area. At other control centers, supporting equipment was tampered with to slow recovery operations. These appear to be exploratory elements of a campaign that was as much about learning as causing a single blackout.« (Park und Walstrom 2017)

Hinzu kommt, dass die Gruppierung in der Lage war, für den zweiten Stromausfall Ende 2016 eine erneuerte maßgeschneiderte Malware-Version zu entwickeln, genannt »*Industroyer*«. Diese profitierte in ihrer Funktionsweise von den zuvor gesammelten Informationen über die anvisierten Netzwerke und ihre verwendeten Protokolle:

> »With built-in knowledge of communication protocols used in electric grid equipment Industroyer can directly control remote equipment without having to rely on the software grid operators use.« (Park und Walstrom 2017)

Die BlackEnergy-Malware stammte ursprünglich aus der Cyberkriminalität und kam bereits 2007 zur Anwendung. Sandworm integrierte die Malware in sein Portfolio, nutzte sie 2014 mutmaßlich als alleiniger Akteur und passte dessen Funktionsweise zur Infiltration der Steuerungsanlagen kritischer Infrastrukturen als BlackEnergy3-Version an (Baumgartner und Garnaeva 2014). Eine Schlussfolgerung lautet, dass Sandworm aus dem Cyberkriminalitätssektor stammt, mit diesem zusammenarbeitet oder lediglich von dessen Angriffs-Tools profitiert hat. Für die zweite Option spricht, dass vereinzelten Quellen zufolge Sandworm für die DDoS-Angriffe auf Georgien 2008 mitverantwortlich gewesen sei (CFR 2021),[87] genau wie das zeitweilig den internationalen Cyberkriminalitätssektor dominierende RBN (Sambaluk 2019, S. 84–85).

Sandworm ist eine von zwei russischen Proxy-Gruppierungen, die mittlerweile dem Militärgeheimdienst GRU und dessen Einheit 74455, auch bekannt als das ›Main Centre for Special Technologies‹ (GTsST), zugeordnet werden, z.B. seitens der USA in einer Anklage aus 2020. Darin werden die angeklagten Hacker als Mitglieder Sandworms sowie GRU-Offiziere benannt (DoJ 2020c). Eine konkrete Verbindung zwischen Sandworm, der Malware BlackEnergy sowie Russland als mutmaßlichem Sponsor stellte der ukrainische Geheimdienst SBU erstmals im Rahmen des ukrainischen Stromausfalls 2015 her. Dies geschah in Kombination mit den Erkenntnissen diverser IT-Unternehmen (iSight Partners, ESET, Dragos; Brewster 2016b). Das Angriffsprofil Sandworms stützt die These der GRU-Affiliation, wird davon ausgegangen, dass der Militärgeheimdienst eines Landes besonders im Rahmen bewaffneter Konflikte auch im Cyberspace operativ bzw. be-

87 Die seitens des CFR Trackers zu diesem Vorfall verlinkten Quellen enthalten jedoch keinerlei Verweise auf Sandworm oder deren alternative Bezeichnungen. Stattdessen wird zeitweilig auch Fancy Bear/APT28 mit den DDoS-, und auch Phishing-Operationen in Verbindung gebracht (Beuth et al. 2017; Guarnieri 2015). Erklären ließe sich dies durch die gemeinsame GRU-Affiliation der Proxy-Gruppen, die eine für frühere Operationen diffizile Unterscheidung erschwerte. Für die Fancy-Bear-Attribution sind die Datumsangaben besagter Spearphishing-Operationen gegen das georgische Innenministerium teilweise jedoch widersprüchlich (siehe FireEye 2014, S. 7 vs. Guarnieri 2015).

auftragend tätig sein dürfte. Dem GRU wird auch im allgemeinen Bereich ein eher weniger subtiles, »*aggressive and risk-taking*« Operationsvorgehen attestiert (Galeotti 2016b, S. 2), was, wie aufgezeigt, auch im Cyberspace der Fall ist.

Abschließend werden die russischen Proxy-Gruppierungen Gamaredon sowie Dragonfly/Energetic Bear vorgestellt:

Die Gruppe Gamaredon wurde bereits 2015 vom ukrainischen Geheimdienst als mit dem FSB affiliiert attribuiert (Lewis 2015). Dieser Zuweisung schlossen sich in der Folge IT-Unternehmen an (Lewis 2015), ohne dass dabei jedoch geklärt wurde, ob es sich um ›state-ordered‹- oder ›state-integrated‹-Operationen handelte, die sich in allen drei Fällen gegen die Ukraine richteten und einen militärischen Fokus aufwiesen, etwa im Fall der 2018 gegen ukrainische Regierungsbehörden eingesetzten Backdoor »*Pterodo*« (Gallagher 2018). Aufgrund der zeitlichen Überschneidung mit der militärischen Auseinandersetzung in der Meerenge von Kertsch konnte in deren Zusammenhang eine militärische Zielsetzung vermutet werden.

Das ukrainische SSU Cyber Security Department spezifizierte die genaue Identität der Gamaredon-Mitglieder im November 2021, indem es die Gruppe als »*crimean*« FSB-Offiziere benannte (zitiert in: Lakshmanan 2021). Diese Attribution spricht gegen die Proxy- und für eine stärker direktstaatliche Atttribution.

Die Gruppe Dragonfly/Energetic Bear wurde zunächst als russische Proxy-Gruppierung attribuiert, im weiteren Verlauf jedoch vor allem seitens der US-Regierung als stärker direktstaatlich attribuiert. Dies geschah im Rahmen einer Warnung der 2018 geschaffenen Behörde Cybersecurity & Infrastructure Security Agency (CISA), in der von »*Russian Government Cyber Activity*« die Rede ist (CISA 2018). Der darin beschriebene Spionage-Fokus der Gruppierung gegen die »*energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors*« spiegelt sich auch in der Zielzusammensetzung der drei im HD-CY.CON der Gruppe zugesprochenen Operationen wider.

5.4.2 Russlands Cyberakteursumwelt

Bereits früh betraute Russland staatliche Einheiten mit der zunehmend im Cyberspace verorteten ›Informationskriegsführung‹. Flankiert wurden diese institutionellen Maßnahmen durch Doktrinen und Sicherheitskonzepte des Außenministeriums, in denen die russische Perspektive auf den Cyberspace als Konfliktaustragungsraum zunehmend zum Ausdruck kam. Beispiele hierfür sind u.a. das in Tabelle 16 gelistete ›Nationale Sicherheitskonzept‹ aus 2000 sowie die Militärdoktrinen aus 2010 und 2014. Auf institutioneller Ebene zeichnete sich noch Ende der 1990er Jahre die Federal Agency for Government Communications and Informations (FAPSI) als eine Art russische NSA aus, deren Befugnisse im Bereich der Kontrolle der inländischen Informationssphäre, aber auch der Überwachung und Spionage, im Jahr 2003 jedoch dem FSB übertragen wurden (Giles 2011, S. 52–53).

Bei der für den Aufbau eigener Cybereinheiten notwendigen Integration technisch talentierten Personals, etwa UniversitätsabsolventInnen, mussten die russischen Behörden jedoch nicht nur mit dem russischen, sondern vor allem dem internationalen Privatsektor konkurrieren (Cheravitch und Lilly 2020, S. 35). Im universitären und allgemeinen Bildungsbereich ermöglichten Informatik-Studiengänge sowie HackerInnen-

Schulen die Ausbildung technisch versierter AkteurInnen, deren Finanzierung dabei oftmals von staatlichen Behörden übernommen wurde und wird (Mshvidobadze 2011). Andererseits demonstrieren international anerkannte IT-Unternehmen wie Kaspersky oder IB-Group sowie überwiegend domestisch operierende Technologieunternehmen, wie sie in den beiden Department of Treasury (DoT)-Anklageschriften der USA aus 2018 und 2021 gelistet wurden (DoT 2018; DoT 2021), dass auf privatwirtschaftlicher Ebene AkteurInnen und Kapazitäten prinzipiell vorhanden waren, um trotz ebenfalls vorhandener staatlicher Kapazitäten im Cyberspace Proxys einsetzen zu können. Die Stärkung der heimischen IT-Landschaft wurde vor allem in Folge der Sanktionen gegen Russland aufgrund der Annexion der Krim fokussiert, um weniger abhängig von ausländischen Exporten im Technologiebereich zu sein (Cheravitch und Lilly 2020).

Die Entwicklung russischer High-Tech-Exporte könnte in Verbindung mit den beschriebenen domestisch fokussierten Technologie-Unternehmen der DoT-Sanktionen auf eine vornehmlich inländische Nutzung sehr wohl vorhandener nationaler Technologien Russlands hindeuten. Deren Proxy-Potenziale könnten somit bewusst im eigenen Land behalten oder deren Tätigkeiten durch die eingeschränkte Internationalisierungsstrategie bewusst fernab der weltweiten Öffentlichkeit belassen werden. Ein weiterer Mehrwert für eine mögliche Proxy-Nutzung könnte sein, dass weniger global agierende Unternehmen auch geringerem Druck durch ausländische Regierungen ausgesetzt sind, diesen gegenüber somit eine geringere Interdependenzvulnerabilität aufweisen.

Die nach dem Ende der UdSSR plötzlich arbeitslosen WissenschaftlerInnen und MathematikerInnen fanden jedoch nicht nur im Privatsektor, sondern auch in der Cyberkriminalität neue Beschäftigung (Ilievski und Bernik 2016, S. 14). Somit bestand auch hier ein potenzieller Proxy-Pool für den russischen Staat, insbesondere im Falle fehlender Strafverfolgung im Tausch für Proxy-Handlungen. Sowohl für direktstaatliche als auch Proxy-Operationen war und ist es somit zentral, einen verstärkten ›Brain-Drain‹ technisch versierter Personen zu verhindern und so gleichzeitig die Grundvoraussetzung für Russlands künftige Wettbewerbsfähigkeit im Cyberspace zu schaffen. Dabei könnte das Land vermehrt auf kostenintensivere Technologien, etwa Quantencomputer oder künstliche Intelligenz, angewiesen sein, um die eigenen Ziele zu erreichen (Cheravitch und Lilly 2020). Das Ausbilden von AkteurInnen, die nicht nur niedrigschwellige Angriffe durchführen können, sondern auch zu komplexeren Operationsformen in der Lage sind, konditioniert für die Zukunft noch stärker als bisher das Ausmaß, in dem Russland bei Bedarf auf direktstaatliche oder Proxy-AkteurInnen zurückgreifen kann bzw. muss.

Zusammengefasst konditionierte die russische Cyberakteurslandschaft Anfang der 2000er Jahre die russische Präferenzkonstellation dahingehend, dass diese für außenpolitische Handlungen im Cyberspace grundlegend direktstaatliche, vor allem aber auch die für Russland aufgezeigten Proxy-Operationen ermöglichte. Besonders der Bereich der Cyberkriminalität stellte bereits früh einen wichtigen Proxy-Pool dar. Die seit 2021 vermehrt geführten Debatten um Russlands Verantwortung gegenüber den Handlungen einheimischer Cyberkrimineller, etwa im Rahmen von Ransomwareoperationen, lassen darauf schließen, dass dies auch heute noch der Fall ist (Hunnicutt 2021). Das zunehmend professionell und unternehmerisch anmutende Auftreten besagter Ransomware-Gruppierungen könnte jedoch auf eine Selbstermächtigung der Gruppierungen über die Zeit hindeuten, begünstigt durch ihren finanziellen Erfolg. Die Verhaftung von Mit-

gliedern der REvil-Ransomwaregruppe im Januar 2022 durch den FSB auf Anfrage des FBI könnte als Indiz gewertet werden, dass dies nicht immer im Sinne des Kremls ist (Balmforth und Tsvetkova 2022). Andererseits werteten BeobachterInnen das Vorgehen der russischen Behörden jedoch auch als bewussten Verhandlungsschachzug im Rahmen des sich damals abzeichnenden Aufflammens des Krieges gegen die Ukraine. Der IT-Experte Dmitri Alperovitch bezeichnete die Episode gar als »*Ransomware Diplomacy*« (Marks 2022), die den Status der Cyberkriminellen als Verfügungsmasse der Behörden veranschauliche.

Tabelle 17 listet die jeweiligen Ausprägungen der NCPI-Teilindikatoren auf.

Tabelle 17: Russlands Cyber-Akteursumwelt auf staatlicher/privatwirtschaftlicher Ebene

NCPI-Teilindikatoren *(staatliche Ziele)*	Ausprägung/Schwerpunkt
Cyber (related) Military Doctrines* *(Offense)*	Nationales Sicherheitskonzept 2000: Holistisches Verständnis des Begriffs ›Information-War‹, technische und psychologische Ebene (MOFA 2000) Informationssicherheitsdoktrin 2000 und 2016: Stärkung der Bedrohungsperzeption von ›Information-Threats‹ im Rahmen bewaffneter Kriege (MOFA 2016) Militär-Doktrin 2010, überarbeitet in 2014: Betonung des Stellenwertes nicht militärischer/informationeller Konflikt-austragungsmittel (MOFA 2010) »*Concept on the Activities of the Armed Forces of the Russian Federation in the Information Space*« des Verteidigungsministeriums aus 2011: Ausdifferenzierung der russischen Vorstellung von ›Information-Warfare‹ (MOD 2011) Foreign Policy Concept 2013: IT als militärische Kapazität, um andere Staaten zu beeinflussen (MOFA 2013)
National Cyber Command/Cyber Military Staffing *(Offense)*	*Militär:* ›Information-Troops‹ nach dem Georgien-Feldzug 2008 diskutiert (Giles 2011), 2012 für 2014 angekündigt, in der Zwischenzeit immer wieder dementiert und 2017 schließlich offiziell verkündet (Interfax 2017), zudem: 6th Directorate des GRU (Välisluureamet 2018, S. 55) *Zivile Geheimdienste*: »Special Communications and Information Service« des FSO, seit 2003 Nachfolger der FAPSI (Carr 2011, S. 235), zudem: 16th und 18th Centre des FSB (Välisluureamet 2018, S. 55) Jedoch kein offizielles Cyber-Command wie im Falle der USA ab 2010 vorhanden

Global Top Technology, Cybersecurity Firms *(Offense, Commercial Gain, Intelligence)*	*International agierende IT-Unternehmen (u.a.)* Kaspersky Lab, seit 1997 IB-Group, seit 2003 *Domestisch konzentrierte IT-Unternehmen (u.a.)* (DoT 2021) ERA Technopolis; Pasit, AO (Pasit); Federal State Autonomous Scientific Establishment Scientific Research Institute Specialized Security Computing Devices and Automation (SVA); Neobit, OOO (Neobit); Advanced System Technology, AO (AST) und Pozitiv Teknolodzhiz (Positive Technologies)
High-Tech-Exports *(Offense, Commercial Gain, Intelligence)*	Leichter, kontinuierlicher Anstieg seit 2007 (von 7,2 zu 13,0 Prozent in 2019 am Gesamtexportaufkommen des Landes (World Bank 2021a) Relativ zum Anteil der chinesischen und vietnamesischen High-Tech-Exporte am nationalen Gesamtexport-Geschäft jedoch weitaus geringer (Vietnam hinter Nordkorea auf Platz 5 der proxynutzenden Autokratien)

(Eigene Darstellung)
* Die oftmals als »Gerassimov-Doktrin« bezeichnete Rede des Chefs des Generalstabes der Streitkräfte der Russischen Föderation, Walerij Gerassimov, aus dem Jahr 2013 wird an dieser Stelle nicht aufgeführt, da es sich nicht um eine offizielle Staatsdoktrin handelte und auch in keiner sonstigen Doktrin oder programmatischen Schrift darauf verwiesen wird (Galeotti 2019, S. 158).

5.4.3 Russlands domestische Präferenzkonstellationen und der Einfluss des allgemeinen Konfliktniveaus

Russland nutzte Proxys bislang umfassend zur Durchführung von Cyberoperationen, denen, wie aufgezeigt, unterschiedliche Funktionen im Rahmen varianter politischer Umfelder zukamen. Die Durchführung direktstaatlicher Cyberoperationen wurde im Laufe der Jahre, insbesondere in Folge der Ukraine-Krise, intensiviert. Auch wenn für die meisten der genannten Proxy-Gruppierungen (vor allem Fancy Bear und Sandworm) weitgehend unklar bleibt, ob diese von Anfang an tatsächliche Agenten des Staates waren und nur als Proxys attribuiert wurden oder zunächst unabhängig agierten und im Laufe der Jahre unter immer direktere Kontrolle und Anleitung der Behörden gerieten, wird grundlegend ein im Laufe der Jahre gestiegenes Kontrollniveau der eingesetzten Cyberproxys angenommen. Dies spiegelt sich jedoch nicht im zeitlichen Verlauf der kodierten Proxy- vs. allgemeinen/direktstaatlichen Cyberoperationen Russlands wider, die weitgehend im Einklang miteinander stetig steigend verzeichnet wurden (Abbildung 29). Grund hierfür könnte entweder eine nicht ausreichend distinkte Attributionspraxis der jeweiligen AkteurInnen sein oder eine zumindest für die attribuierten Proxy-Operationen erfolgreiche Verschleierungstaktik Russlands. Diese könnte auch private IT-Unternehmen oftmals zögern lassen, eine APT als direktstaatlichen russischen Akteur zu benennen. Dass für eine Nutzung ›echter‹ Cyberproxys von Beginn des Untersuchungsraumes an die notwendigen Voraussetzungen vorhanden waren, wurde im vorherigen Kapitel demonstriert. Nun gilt es, die beschriebenen Cyberoperationen russischer AkteurInnen sowie deren aufgezeigte institutionellen Hintergründe durch die Ausprägung der domestischen Präferenzkonstellationen des Landes auf allen drei Liberalismus-Ebenen zu erklären bzw. auch auf verbleibende Widersprüchlichkeiten

und somit potenzielle Schwächen des Erklärungsmodells hinzuweisen. Integriert wird hierbei wie im Falle Chinas der Einfluss der IV.

5.4.3.1 Das Who's Who der russischen Winning Coalition

Um russische Außenpolitik im Cyberspace aus liberaler Sicht erklären zu können, bedarf es einer Analyse der hierfür primär relevanten domestischen Akteursgruppierungen, die gewissermaßen am Anfang und Ende des defizitären, autokratischen Transmissionsriemens stehen. Zudem gilt es, deren Interessenvermittlung gegenüber der Regierung zu charakterisieren, ob diese z.B. über institutionalisierte, formalisierte oder personalisierte, informelle Kanäle entsprechend dem republikanischen Liberalismus erfolgt.

Die russische Föderation wird als »*gelenkte Demokratie*« (Mommsen und Nußberger 2007), »*elektorale Autokratie*« (Tertytchnaya 2020), »*kompetitives, autoritäres Regime*« (Buckley und Reuter 2019), »*hybrides Regime*« (Hale 2011) und insbesondere seit Putins zweiter Amtszeit immer häufiger auch als »*personalistisches Regime*« bezeichnet (Fish 2017). Gemäß der Typologie von Kailitz kann Russland unter Putin am ehesten als eine Mischform aus elektoraler Autokratie mit zunehmender Personalisierung bezeichnet werden. Nachdem Putin zu Beginn seiner Präsidentschaft großen Wert auf die Generierung wirtschaftlicher Output-Legitimität legte, nahm der diffuse Aspekt seiner persönlichen Legitimation als ›Strong Man‹ in der Folge eine immer stärkere Rolle ein. Dies zeigte sich vor allem in Zeiten außenpolitischer Krisen wie dem zweiten Tschetschenien- und dem Krieg gegen die Ukraine.

Putins kompromissloses Vorgehen konnte (zumindest zeitweilig) die negativen Auswirkungen seiner Politik (z.B. Wirtschaftssanktionen) ausgleichen, stiegen doch seine Umfragewerte in Folge besagter Militärinterventionen stark an (Interfax 2015). Auch dem Aspekt der Maskulinität schrieben Beobachter eine wichtige Bedeutung in der Putinschen Legitimationsstrategie zu (Sperling 2016). Der Modus der Interessenvermittlung wurde seit Putins Amtsübernahme ebenfalls als zunehmend personalisiert bezeichnet, in dem z.B. Unternehmerverbände, in Demokratien oftmals wichtige Interessengruppen, allenfalls Mittel zum Zweck bzw. ›Machtressourcen‹ der eigentlichen Teile der nachfolgend behandelten Winning Coalition darstellen (Stykow 2006, S. 31).

Nach dem Ende der Amtszeit von Boris Jelzin und somit vor Beginn der Putin-Ära Ende der 1990er Jahre befand sich das Land in einem tiefgreifenden Reformprozess, der durch Jelzin in Folge des Zerfalls der Sowjetunion initiiert wurde. Dabei kam es zu Marktliberalisierungen, Privatisierung und letztlich steigender Macht der sog. Oligarchen auch im politischen System (Desai 2005, S. 96). Auf politischer Ebene wurde Russland in der 1993 verabschiedeten und im Kern bis heute gültigen Verfassung als »*demokratischer, föderaler Rechtsstaat mit republikanischer Regierungsform*« mit umfassenden politischen Rechten für den Präsidenten definiert. So obliegt es diesem etwa (mit Zustimmung der Duma), den Ministerpräsidenten zu ernennen, er darf die Regierung einberufen und entlassen, die nur ihm und nicht dem Parlament rechenschaftspflichtig ist, er kann Dekrete erlassen und ist oberster Befehlshaber der Streitkräfte. Duma und Föderationsrat wurden im Laufe der Jahre durch Putin sogar noch weiter entmachtet, z.B. in Folge einer Wahlreform sowie durch das eingeführte Recht des Präsidenten, zusätzlich zehn Prozent des Föderationsrates selbst zu bestimmen (Schröder 2018). Die unter Jelzin noch weitaus mächtigeren Gouverneure der Föderationen wurden im

Rahmen der ›Vertikale der Macht‹ unter Putin politisch geschwächt, das Modell der ›souveränen Demokratie‹ wurde weiter ausgebaut (Chepikova und Leiße 2010). Die domestische Interessenvermittlung wurde immer weiter auf den Kreml zugeschnitten, politische Parteien existieren zwar formal und sind in der Duma vertreten, wurden jedoch in der Verfassungswirklichkeit durch die Dominanz der Putin-Partei ›Einiges Russland‹ zunehmend marginalisiert, zu einem wirklichen Parteienwettbewerb kam es daher nicht mehr (Gel'man 2008). Nichtsdestotrotz wurde auch das Verhältnis zwischen Einiges Russland und dem Kreml als nicht konfliktfrei beschrieben, was de facto das Spannungsverhältnis zwischen Exekutivdominanz und zumindest in der Verfassung formal angelegtem Parteiensystem auf republikanischer Ebene verdeutlicht (Sakwa 2012).

Als zentraler Teil der autokratischen Winning Coalition seit 2000 und somit dem Beginn des Untersuchungszeitraumes können die sog. ›Silowiki‹ betrachtet werden. Dabei handelt es sich zumeist um ehemalige KGB-Mitglieder und nun russische Geheimdienstangehörige mit oft engen Beziehungen zur nationalen Rüstungsindustrie, aus der sich auch in erster Linie der engste Kreis aus mit Putin vertrauten Regierungsoffiziellen speist (Markus 2017, S. 105).

Den gemeinhin als Oligarchen bezeichneten WirtschaftsakteurInnen kommt im Gegensatz zur Jelzin-Ära dagegen verstärkt die Rolle des ›Juniorpartners‹ zu: Im Rahmen einer umfassenden »*anti-oligarchic campaign*« (Sakwa 2008, S. 188) u.a. gegen Boris Beresowski und Michail Chordorkowski, kehrte Putin die vormalige Machtasymmetrie zu Gunsten seiner Stellung als Präsident um. In der Folge hatten sich Oligarchen weitgehend aus der Politik herauszuhalten, während sich die Politik umfassend in deren Geschäftstätigkeiten einmischte und so die staatliche Kontrolle über das russische Wirtschaftssystem etablierte (Sakwa 2008, S. 188). Zwar formulierten einzelne Oligarchen auch in den letzten Jahren immer wieder eigenständige Forderungen, etwa nach verbesserten Beziehungen zum Westen, konnten diese aufgrund ihrer Abhängigkeit vom Putin-Regime und dem gegenseitigen Konkurrieren um ›Rents‹ jedoch bislang nicht durchsetzen (Markus 2017). Der Begriff der ›Silovarchy‹ bringt zum Ausdruck, wie frühere Oligarchen aus der Jeltsin-Ära, etwa Beresowski, Chordokovski oder Wladimir Gusinsky, zunehmend aus der Politik gedrängt wurden und oftmals nur in das Exil flüchten konnten. Gleichzeitig wurden immer mehr wichtige Führungsposten russischer Staatskonzerne (z.B. Rosneft) durch Silowiki besetzt, wodurch die »*Silovarchy*« begründet wurde (Treisman 2007, S. 142).[88] Die Gruppe der Silowiki wuchs beständig, so verdoppelte sich die Anzahl der Staatsunternehmen Russlands im Zeitraum von 2013 bis 2016 (Fish 2017, S. 71). ›Reine‹ Oligarchen wurden bislang nicht als realistische Gegenspieler Putins angesehen, auch, da ihnen zumeist die Bindung zur breiten Bevölkerung fehlte und sie zu keiner koordinierten Anstrengung im Stande waren (Markus 2017, S. 108). Daher werden ihre Interessen nachfolgend nicht gesondert analysiert.

Darüber hinaus wird in der Literatur häufig von Putins ›innerem Zirkel‹ gesprochen, der aus Silowiki, aber auch ehemals liberalen Anwälten oder Ökonomen wie

88 Rutland verweist 2018 auf die oftmals unklare Trennung zwischen Putins innerem Kreis, Oligarchen sowie Silowiki, die oftmals überlappende Tätigkeitsfelder aufweisen.

Dmitri Medwedew zusammengesetzt ist (Rutland 2018, S. 284). Daher werden deren Interessen nochmals getrennt behandelt.

Auch Teile des Militärs werden den Silowiki zugerechnet und stellen somit eine wichtige Stütze des Regimes, nicht zuletzt im Rahmen gewaltsamer Konflikte wie dem Krieg gegen die Ukraine und dem Syrienkonflikt, dar. Dabei wurde zu Beginn der Putin-Ära gar von »*Putin's Militocracy*« gesprochen (Kryshtanovskaya und White 2003). Letztlich stehen jedoch auch die Streitkräfte unter Putins direkter Kontrolle, dem auch im Außen- und Sicherheitsbereich die finale Entscheidungsgewalt obliegt (Finch III 2018). Sogar der Partei Einiges Russland wird dagegen eine geringere Bedeutung für den Zugang zum hochgradig informellen politischen Netzwerk im Vergleich zu einer Geheimdienst-Biografie/Zugehörigkeit zugesprochen. Gleiches gilt auch für das weitgehend machtlose Parlament, die Duma (Mommsen 2018). Zuletzt wird auch der russisch-orthodoxen Kirche seit Putins dritter Amtszeit ein erheblicher Einfluss im politischen System attestiert.[89] Inwiefern deren Interessen jedoch tatsächlich Einfluss auf die russische Cyberstrategie gehabt haben könnten, gilt es im Folgenden zu diskutieren.

Zusammengefasst sticht ein Befund auf republikanischer Ebene heraus: Putin schaffte es im Laufe der Jahre, unterschiedliche AkteurInnen der Winning Coalition politisch zu entmachten, aus dem Land zu vertreiben oder zu kooptieren. Einzig Oppositionelle, wie der seit 2021 inhaftierte Alexey Nawalny, die stärker dem Zivilsektor zuzurechnen sind, vermochten es zuletzt auf domestischer Ebene eine Art ideellen Gegenpol zu Putin und dessen Eliten zu bilden. Er und seine AnhängerInnen erhielten insbesondere infolge der Massenproteste um angebliche Wahlmanipulationen im Rahmen der Präsidentschaftswahl 2012 immer mehr Zuspruch (Schepp 2013). Der Herrschaftszugang dieser Opposition außerhalb des politischen Systems wurde jedoch auf institutioneller Ebene weitgehend eingeschränkt, etwa durch das Verbot für Nawalny, an den Präsidentschaftswahlen 2018 teilzunehmen. Dass dessen Präferenzen jedoch als immer gefährlicher für die Sicherheit des Regimes angesehen wurde, verdeutlicht der Nowitschok-Giftanschlag auf Nawalny 2020, der dem russischen Geheimdienst FSB zugesprochen wurde (Deutsche Welle 2020). Anfänglich noch als nationalistischer Anti-Korruptionskämpfer auftretend, verband Nawalny in der Folge nationalistische und liberale Forderungen und mobilisierte so im Vergleich zu anderen Oppositionellen weitaus effektiver AnhängerInnen in der russischen Bevölkerung (Mangott 2012). Nawalny wird somit nicht als Teil der Winning Coalition, sehr wohl aber als relevant für deren Präferenzordnung angesehen, insbesondere für Putin selbst sowie die Hardliner des Regimes.

Der Herrschaftszugang der einzelnen Gruppierungen der Winning Coalition ist mit der Zeit immer abhängiger vom personalistischen System und somit von Putin selbst geworden. Daher werden zunächst dessen eigene Präferenzen auf ideeller und kommerzieller Ebene herausgearbeitet. Nichtsdestotrotz sollen auch mögliche Einflussfaktoren verschiedener Elitengruppierungen, allen voran der Silowiki, explizit miterfasst

89 Diese Einschätzung bestätigt auch ein Brief von Boris Beresowski an den Vorsteher der russisch-orthodoxen Kirche, er möge Putin zur Vernunft bringen und diesen zu Gunsten des Volkes entmachten (Achmatova 2012).

und in Bezug auf die dargestellte russische Cyberproxy-Nutzung analysiert werden.[90] Aufgrund der Zentralisierung der Macht innerhalb der Exekutive entwickelten die verschiedenen Behörden-Bürokratien ein immer stärkeres Konkurrenzstreben um Putins Gunst, das in der Folge laut Beobachtern die russische Außenpolitik oftmals entscheidend mitbestimmte und zu einer zeitweilig hohen Fluktuation in der Besetzung öffentlicher Ämter in Politik und Wirtschaft führte (Bremmer und Charap 2007, S. 84; Harding 2007).[91] Hinzu kommt die Verortung offensiver Cyberoperationen entweder im zivil- oder militärgeheimdienstlichen Geschäftsbereich, ein weiterer Grund für die besondere Relevanz der Silowiki.

5.4.3.2 Putins Silowiki – zwischen Großmachtstreben und politischer Stabilität

> »I was an officer for almost twenty years. And this is my own milieu.… I relate to individuals from the security organs, from the Ministry of Defense, or from the special services as if I were a member of this collective.«
> *Wladimir Putin, zitiert in Rivera und Rivera (2018, S. 221)*

Das voranstehende Zitat verdeutlicht Wladimir Putins Sozialisation und Identifizierung mit den Geheimdienst- und Sicherheitsorganen Russlands bzw. zuvor der UdSSR. Aus diesem Grund werden Putins Präferenzen gemeinsam mit denen der Silowiki behandelt. Ihnen werden zeitgleich der größte Herrschaftszugang im russischen System und somit die größten Interessensdurchsetzungschancen auch mithilfe von Cyberoperationen attestiert.

Als Silowiki zu nennen wäre etwa Igor Sechin, der von 1999 bis 2008 stellvertretender Stabschef Putins war. In dieser Rolle hatte er ein hohes Maß an Kontrolle über den Terminkalender des Präsidenten und bestimmte aktiv mit, wer welchen Zugang zu ihm erhielt und wer nicht (Bremmer und Charap 2007, S. 87). Nachdem er zwischenzeitlich unter Medwedew eine Art Degradierung erfahren hatte, bekleidete er in der Folge führende Positionen im Staatsunternehmen Rosneft und wurde 2017 nach wie vor als zweitmächtigster Mann Russlands angesehen (Walker 2017). Des Weiteren zählten bislang folgende Personen zu Putins innerstem ›Silowiki-Kreis‹: Viktor Ivanov, lange Zeit zuständig für personelle Besetzungen sowohl in der Regierung als auch in staatseigenen Konzernen; Alexander Bortnikov, FSB-Chef seit 2008, jedoch Berichten zu Folge nicht nur Putin, sondern auch Medwedjew eng verbunden (Reuters 2011); zuletzt Nikolai Patrushew, FSB-Direktor von 1999 bis 2008 und seither Chef des nationalen Sicherheitsrates mit großem Einfluss auf Russlands Ukraine- und Balkan-Politik (Amos 2017).[92]

Daher werden zunächst die geteilten Interessen von Putin und den Silowiki analysiert. Nachfolgend gilt es, Letztere entsprechend ihrer Subfraktionen zu unterscheiden,

---

90 Den Silowiki wird unabhängig von den graduell unterschiedlichen Eliteneinteilungen in der Forschungsliteratur der größte Herrschaftszugang im russischen System attestiert, auch im Vergleich zu Liberalen, oder Technokraten wie (Medwedjew Bremmer und Charap 2007).

91 Zudem wurde bereits darauf verwiesen, dass Putin zwar prinzipiell alle Entscheidungen final treffen könnte, daran jedoch gar nicht in allen Fällen ein Interesse habe (Noble und Schulmann 2021).

92 Die aufgelisteten Personen repräsentieren die hier behandelten Silowiki, zu denen über Zeit jedoch weitere Akteure gehörten.

um somit den Einfluss der republikanischen Ebene auf den russischen Cyberkonfliktaustrag umfassender analysieren zu können. Trotz geteilter Interessen können die Silowiki nicht als gänzlich einheitliche Akteursgruppe betrachtet werden, insbesondere im Falle konkurrierender Geheimdienstzugehörigkeiten (Galeotti 2015, S. 10).

Die gemeinsamen Präferenzen Putins und der Silowiki können durch drei Prinzipien beschrieben werden, denen auf verschiedenen Ebenen besondere Relevanz für die russischen Cyberoperationen attestiert wird:

Russland als souveräne Großmacht im Rahmen einer multipolaren Weltordnung

Begonnen wird mit dem unter Putin deutlich gewordenen Bestreben des Kremls, Russlands Status als Großmacht auf internationaler Ebene wiederherzustellen, nachdem der Zerfall der UdSSR das Land geschwächt hatte. Damit einhergehend war auch die Stärkung der eigenen Souveränität infolge der fehlenden Anerkennung seitens liberal-demokratischer Großmächte das Ziel (Clunan 2019, S. 3).[93] Länder wie die USA wurden als »*Russia's strategic benchmark, the yardstick against which Russia compares itself*« bezeichnet. Putin sei zudem getrieben »[…] *by his vision of Russia as a great power operating according to the logic of par in parem non habet imperium (›an equal has no authority over an equal‹)*« (Herd 2019, S. 25). Die Perzeption der USA als feindlich gesinnte, hegemoniale Großmacht, die Russlands Souveränität zu untergraben versuche, spiegelt sich auch in der Äußerung Patrushews wider: »*They* [die USA; Anmerkung der Autorin] *would much rather that Russia did not exist at all. As a country*« (Chernenko 2015).

Im russischen Großmachtstreben drückt sich jedoch nicht nur diese unter Putin auf die Spitze getriebene Aversion gegen jegliche Formen von US-Hegemonie nach dem Ende des 20. Jahrhunderts aus, sondern auch eine Art ›Kampf der Systeme‹: Nachdem während des Kalten Krieges auf ideeller Ebene insbesondere der Konflikt zwischen liberalem Kapitalismus und sowjetischem Kommunismus im Vordergrund stand, bezog sich das Spannungsverhältnis nach dem Ende der dritten Demokratisierungswelle und steigender Autokratisierungstendenzen immer stärker auf den Gegensatz zwischen liberalen Demokratien und autoritär geführten Staaten (Merkel 1999, S. 174). Putin und seine Chefideologen, allen voran Wladislav Surkov, erklärten bereits seit Beginn der 2000er Jahre, dass das russische System eine besondere Form der Demokratie darstelle, entsprechend der nationalen Charakteristika des Landes. Dies führte zur Prägung von Begriffen wie der ›gelenkten‹ oder auch der ›souveränen Demokratie‹, um illiberalen Maßnahmen auf republikanischer Ebene eine ideell-begründete Legitimation verleihen zu können (Lipman 2006).

Die Vorstellung einer notwendigen Zentralisierung aller Staatsgewalt in den Händen der Exekutive zum Wohle des Erhalts der Einheit und Souveränität des russischen

93 Verantwortlich hierfür war eine Art Umdeutung des Souveränitätskonzeptes, das immer stärker auf Vorstellungen von »*good governance*«, z.B. dem Schutz der Rechte der BürgerInnen sowie ökonomischer Performanz beruhte (Clunan 2019, S. 3). Durch die weltweite Verbreitung liberaler Werte definierte sich die staatliche Status-Hierarchie immer weniger über materielle Hardpower-Ressourcen und immer stärker über die Qualität innerstaatlicher Demokratie (Pouliot 2014 & 2016), was das russische Selbstverständnis einer ›Great Power‹ ernsthaft bedrohte.

Staates wurde zu einer Hauptmaxime des Kremls (Clunan 2019, S. 4). Politische und ökonomische Stabilität seien liberalen Vorstellungen von Gewaltenteilung und Partizipation strikt vorzuziehen. Das Gleiche gelte nicht nur für liberal-demokratische Prinzipien auf republikanischer, sondern vor allem auch auf ideeller Ebene: So sei die liberale Wertediktatur des Westens, in der etwa Gleichberechtigung für verschiedene Minderheiten gefordert wird, mit der russischen Kultur nicht vereinbar, weshalb es unter Putins Präsidentschaft etwa keine gleichgeschlechtlichen Ehen geben werde (Reuters 2020a). Putin kritisierte zudem wiederholt die aus seiner Sicht gegebene Abkehr der EU von traditionellen christlichen sowie familiären Werten, was seiner Charakterisierung Russlands als ›konservativer‹ Macht entspricht (Tsygankov 2019, S. 45–46). Zugleich stellte er die Gemeinsamkeiten der orthodoxen russischen Kirche mit den Werten des Islams als größer dar als etwa im Vergleich zu westlichen ProtestantInnen (Alekseyeva 2015). An dieser Stelle kann jedoch gleichzeitig der vielleicht überraschende Befund vorweggenommen werden, dass Russland unter Putin immer wieder den Anspruch auf ein bewusst multiethnisches Nationenverständnis zum Ausdruck bringt (Kremlin.ru 2012), was jedoch im Kontext des nachfolgend behandelten ›nahen Auslands‹ interpretiert werden muss.

Die auf ideeller Ebene immer stärkere Abgrenzung von liberalen Demokratien und deren Wertvorstellungen mit korrespondierenden Autokratisierungsprozessen auf institutioneller Ebene unter Putin wie der systematischen Zentralisierung der Staatsgewalt sowie der Entmachtung potenzieller VetospielerInnen im System (Duma, Parteien, Gerichte, Regionen, Medien, Oligarchen) kann dabei einen erheblichen Anteil der verzeichneten russischen Cyberproxyoperationen erklären. Hinzu kommt, dass diese Bedrohungsperzeption ein geteiltes Narrativ Putins und der im Rahmen der ›Vertikale der Macht‹ begünstigten AkteurInnen der Sicherheitsorgane darstellt. Mithilfe bestimmter Cyberoperationen konnte die exklusive Durchsetzung ihrer geteilten Interessen auf vor allem ideeller Ebene verfolgt werden. Dabei handelt es sich um diejenigen Vorfälle, die sich gegen liberale Demokratien richteten, allen voran die USA, aber auch Deutschland, Großbritannien, Kanada oder Frankreich, sowie die mit diesen assoziierten internationalen Organisationen wie die UN, die WADA und besonders die NATO. Mit diesen Ländern befand sich Russland zum Zeitpunkt der Operationen in keinem gewaltsamen konventionellen Konflikt, was als primäre Erklärung für die Cyberspionage und besonders auch Doxing-Operationen hätte dienen können. Vielmehr kann der beschriebene ideelle Systemkonflikt mit den USA sowie deren liberal-demokratischen Alliierten als Hauptursache hierfür ausgemacht werden. Deren zu Russland konfliktive Präferenzinkompatibilitäten, ausgedrückt durch den Anspruch auf ideelle Diskurshoheit, allen voran im Bereich der Menschenrechte sowie des Selbstbestimmungsrechts der Völker, führte im Laufe der Jahre zu immer stärkeren Interdependenzvulnerabilitäten auf russischer Seite. Diese drückten sich besonders im liberal-demokratischen Engagement zur Unterstützung russischer Oppositioneller, MenschenrechtsaktivistInnen und NGOs aus. Gleiches gilt für die Länder des ›nahen Auslands‹ (Babayan 2015). Dieses Engagement kulminierte aus russischer Sicht in den sog. ›Coloured Revolutions‹ in Georgien, der Ukraine und Kyrgyzstan zwischen 2003 und 2005, dem Arabischen Frühling ab 2010 sowie dem Euromaidan in der Ukraine ab 2013. Kritik am russischen Autoritarismus, z.B. infolge der Präsidentschaftswahlen 2011 durch Hillary Clinton, verstärkten auf russischer Seite die Wahrnehmung zunehmender Verwundbarkeiten auf ideeller Ebene. Ermöglicht

wurde dies auch durch die Interdependenz des russischen Sprachraums mit der internationalen Umwelt. Im Cyberspace zeichnet sich dieser durch ein im Vergleich zu China offeneres Runet aus. Grund hierfür ist u.a., dass die russische Internetentwicklung im Gegensatz zu China staatlichen Repressions- und Kontrollbemühungen vorgelagert war (Troianovski 2021).

Theoretisch gesprochen empfand Russland unter Putin die Interessensdurchsetzung liberaler Demokratien wie der USA im Sinne der Demokratie- und Menschenrechtsförderung als zunehmend konfliktiv zu den eigenen Präferenzen. Da Putin und die Silowiki ihren Herrschaftsanspruch auf dem genauen Gegenteil errichtet hatten, dem autokratischen Versprechen politischer Stabilität, Souveränität sowie der Befreiung vom liberalprogressiven Wertediktum, konnte eine Infiltration des eigenen Landes mit genau jenen Wertvorstellungen der Regimestabilität potenziell nur gefährlich werden. Auch wenn versucht wurde, die Vorzüge des eigenen Systems gegenüber der liberalen Demokratie hervorzuheben, baute der russische Ansatz im Cyberspace zur Verringerung dieser wahrgenommenen Vulnerabilität auf der Unterminierung des gegnerischen Systems im Sinne eines Nullsummenspiels auf (Galeotti 2016b, S. 5). So waren die beschriebenen Doxing-Operationen gegen Institutionen wie die WADA, die zuvor russische Norm-Devianz bzw. Fehlverhalten gegenüber der internationalen Öffentlichkeit offengelegt hatten, auf deren eigene Diskreditierung ausgelegt. So wurden in internen E-Mails Anzeichen für demokratischen Wertevorstellungen entgegenstehende Ansichten oder Verhaltensmuster gesucht und veröffentlicht.

Dieses »*liberal mimicry*« (Bettiza und Lewis 2020), d.h. die Instrumentalisierung demokratischer Prinzipien (z.B. Transparenz) gegen demokratische EntscheidungsträgerInnen selbst, fand seinen zeitweiligen Höhepunkt im Rahmen des DNC-Hacks/Leaks 2016. Offensichtliches Ziel der Operation war es, den Fokus der Debatte im Vorfeld der Wahlen auf die demokratische Partei und deren laut den veröffentlichten E-Mails nicht demokratische Verfahrensprozesse der KandidatInnenauswahl zu legen. Die Botschaft lautete, dass auch Demokratien ihren eigenen Forderungen nach politischer Chancengleichheit regelmäßig nicht nachkommen und somit das Glashaus, in dem sie sich befinden, besser nicht mehr zum Einsturz bringen sollten, indem etwa auf russische Wahlmanipulationen hingewiesen wird. Dabei wurden die auf US-Seite identifizierten Verwundbarkeiten wie die zunehmende Polarisierung zwischen links und rechts, die immer extremere Medienberichterstattung sowie eine steigende Anti-Establishment-Haltung unter Barack Obama konsequent ausgenutzt (Harding et al. 2021). Laut einem vom Guardian im Juli 2021 veröffentlichten internen Regierungsbericht der russischen Seite war die DNC-Operation ein von Putin im Januar 2016 initiiertes Unterfangen. Dabei kamen alle drei Geheimdienste zusammen und erarbeiteten unter Führung des GRU-Chefs Shoigun einen entsprechenden Plan, um Trump zur Wahl zu verhelfen. Diese interne Machtverteilung entspricht auch der prominenten Rolle Fancy Bears als GRU-Ableger im Rahmen des DNC-Hacks. Konkret versprach sich der Kreml laut dem geleakten Papier durch eine sabotierte Wahl Trumps, dass »›*Putin would be able in clandestine fashion to dominate any US-Russia bilateral talks, to deconstruct the White House's negotiating position, and to pursue bold foreign policy initiatives on Russia's behalf*‹« (Harding et al. 2021). Laut weiterer im Guardian-Artikel erwähnter Quellen habe Putin zudem im April 2016 das Leaken der erbeuteten DNC-Mails selbst angeordnet.

Dieses Streben nach der Unterminierung ureigener demokratischer Prozesse, allen voran der Integrität demokratischer Wahlen sowie der Möglichkeit zur freien und unbeeinflussten Meinungsbildung, äußerte sich auch noch in weiteren Cyberoperationen, z.B. den ›Tainted Leaks‹ manipulierter E-Mails des französischen Präsidenten Macron im Vorfeld der Wahlen 2016 (Hulcoop et al. 2017, S. 36), aber auch den berichteten Hacks diverser US-Wahlcomputer-Firmen 2016 (Zetter 2019).[94] Bei Letzteren ging es im Gegensatz zum DNC- und Macron-Leak nicht um das Veröffentlichen kompromittierender Inhalte, sondern um das Untergraben des Vertrauens der Bevölkerung in die technische Wahlinfrastruktur selbst. Für diese intendierte Wirkung war es prinzipiell zweitrangig, ob Stimmen tatsächlich manipuliert werden konnten. Allein die Möglichkeit, dass so etwas möglich gewesen wäre, unterminierte in der Folge die Integrität der US-Wahlen und trug zur weiteren Polarisierung der bereits zuvor auseinanderdriftenden amerikanischen Gesellschaft bei (vgl. Zettl 2019). Derselben Taktik bediente sich in der Folge auch Donald Trump, indem er die Wahl 2020 immer wieder als manipuliert bezeichnete, ohne jedoch konkrete Beweise hierfür geliefert zu haben (Sanchez 2020).

Eine mögliche Anomalie des Leakens gehackter Informationen stellt der Hack des deutschen Bundestages 2015 dar: Nachdem Fancy Bear/APT28 immense Mengen an sensiblen Daten diverser Abgeordneter hatte abgreifen können, wurden in der Folge auch in Deutschland Befürchtungen laut, Teile daraus könnten im Rahmen des deutschen Bundestagswahlkampfes 2017 instrumentalisiert werden (Hummel 2017). Dass dies letztlich nicht der Fall war, kann zum einen an fehlender Brisanz der Daten, wahrscheinlicher jedoch an den anders gearteten Rahmenbedingungen des deutschen Wahlkampfes gelegen haben. So entfalteten diverse Charakteristika des deutschen Systems auf ideeller und vor allem republikanischer Ebene vermutlich eine Resilienzwirkung gegenüber ausländischer Einflussnahme, wie sie Russland hätte anstreben können. Deutschland zeigte sich auf ideeller sowie republikanischer Ebene somit als weniger vulnerabel im Vergleich zu den USA (Zettl 2019).

Den russischen Sicherheitsorganen und somit den ihnen vorstehenden Silowiki werden trotz aller Einigkeit in Bezug auf die Notwendigkeit der Restauration des russischen Großmachtstatus sowie ihrer Loyalität gegenüber Putin Tendenzen zu »*Turf Wars*« attestiert (Galeotti 2015 & 2016a). Die daraus resultierenden überlappenden Einsatzaktivitäten und fehlende Koordination im Sinne eines holistischen Sicherheitskonzepts übertrugen sich auch auf den Cyberspace. Relevant ist dies besonders für den in diesem Abschnitt behandelten DNC-Hack/Leak: Hier waren sowohl der GRU mithilfe der ihm zugeordneten Gruppierung Fancy Bear als auch Cozy Bear und somit mutmaßlich der SWR im selben Zielsystem zeitgleich aktiv. Der erwähnte Guardian-Bericht legt nahe, dass dieses parallele Vorgehen erst ab dem berichteten Treffen Putins mit den Geheimdienstchefs im Januar 2016 zu einer konzertierten Aktion mit dem GRU in der Führungsposition wurde. So hatten Cozy Bear und somit der SWR, wie bereits beschrieben, mit der

94 Russische Cyberoperationen machten jedoch auch vor den eigenen Wahlen nicht halt: So wurden diverse Nachrichtenwebseiten, aber auch die Wahlbeobachtungsinstitution Golos im Vorfeld der Präsidentschaftswahlen 2012 laut betroffenen Organisationen seitens »*state-sponsored criminals*« durch DDoS-Angriffe lahmgelegt (BBC 2012), was als versuchte Störung der Interessensartikulation und oppositionellen Mobilisation gewertet werden kann.

disruptiveren Operationsform des Leakens nichts zu tun, sondern betrieben bereits seit 2015 Spionage im DNC-Netzwerk, bevor 2016 Fancy Bear dazu stieß (CrowdStrike 2020).

Der Anfang 2017 kolportierte Geheimnisverrat der FSB-Akteure könnte Ausdruck des Unbehagens des FSB gegenüber dem Wiedererstarken des GRU in Folge des Georgien-Konflikt 2008 gewesen sein, ermöglicht insbesondere auch durch Cyberoperationen sowie den Ukraine-Konflikt. Die mutmaßliche Gegenreaktion des GRU, besagte FSB-Agenten hierfür des Hochverrats zu beschuldigen, demonstriert dieses ›Tit-for-Tat‹ zwischen den Geheimdiensten. Nichtsdestotrotz sind diese partiell auch in der Lage zu erkennen, wenn sie gegenüber anderen Behörden außerhalb des Geheimdienstsektors gemeinsame Interessen besitzen, wie im Falle der vom Kreml beabsichtigten Besetzung des GRU-Chefpostens durch einen Außenseiter und somit ›Nichtsilowiki‹. Hierbei unterstützte der FSB russischen Quellen zufolge den Widerstand des GRU, wohl wissend, dass dies auch für die eigene Behörde einen ungewollten Präzedenzfall hätte schaffen können (Galeotti 2016b, S. 10).

Der DNC-Hack/Leak könnte somit die Chance zur Wiedergutmachung des GRU gegenüber Putin in Folge des Georgienkonflikts gewesen sein, um die eigene Interessensdurchsetzung zu verbessern (vgl. Galeotti 2015, S. 9). Diese Sichtweise erklärt auch die weiteren Operationen von Fancy Bear, aber auch des zweiten GRU-Ablegers Sandworm, die weitaus stärker vom traditionellen Spionage-Muster abgewichen sind und Sabotage auf physischer sowie psychologischer Ebene immer stärker in ihr Portfolio integrierten. Relevant hierfür ist jedoch besonders das militärische Profil des GRU, das einen stärkeren Hang zu eskalativeren Operationsformen, insbesondere im Rahmen gewaltsamer Konflikte, auch im Cyberspace erklärt.

Das Streben Putins und der Silowiki nach internationaler Akzeptanz Russlands als souveräne Großmacht des 21. Jahrhunderts drückte sich auf der Ebene der kommerziellen Interessen durch eine Art ›souveräne Globalisierungsstrategie‹ des Landes aus (Gould-Davies 2016). Diese sah ein Ausbalancieren des auch im ökonomischen Bereich angestrebten staatlichen Kontrollanspruchs gegenüber wirtschaftlicher Prosperität vor. Dies beruhte vor dem Ukraine-Konflikt in erster Linie auf den nationalen Rohstoffressourcen und der daraus erwachsenen Abhängigkeit europäischer Länder von russischen Öl- und Gasexporten (Protasov 2010). Die Ernennung des Wirtschaftsexperten Michail Fradkow zum damaligen Chef des SWR verdeutlicht die bedeutende Rolle der Geheimdienste auch hierbei, da deren Spionage auch gegen geostrategisch relevante EU-Länder ausgerichtet war (Banse 2009). Die verstärkte Abhängigkeit europäischer Länder von den eigenen Energie-Exporten wurde als zentraler Bestandteil der nationalen Stabilität und letztlich der Regimesicherheit angesehen. Hieran konnten alle Silowiki ein Interesse haben und somit auch an Cyberoperationen, die die ökonomische Interdependenzasymmetrie zu Gunsten Russlands verändern. Zu nennen sind hier die zahlreichen im HD-CY.CON verzeichneten Cyberspionage-Operationen russischer AkteurInnen gegenüber kritischen Infrastrukturen sowie politischen Institutionen osteuropäischer Länder, z.B. deren Außen- oder Wirtschaftsministerien. Diesen Aufgabenbereich teilen sich

FSB, SWR und GRU den Attributionskodierungen nach weitgehend, was als Ausdruck der gemeinsamen Präferenz gewertet wird.[95]

Das vereinte Interesse an wirtschaftlicher Stabilität durch den Erfolg staatlich kontrollierter Energieunternehmen und somit der Umgehung einer umfassenden Liberalisierung der staatlichen Wirtschaft ist für Putin und die Silowiki nicht nur für die Wiederherstellung des eigenen Großmachtstatus, etwa zur Finanzierung militärischer Einsätze wie in der Ukraine oder Syrien, sondern auch für die Stärkung des russischen Regionalmachtanspruchs in Eurasien zentral.

Russland als hegemoniale Regionalmacht in Eurasien

Russlands Streben nach einer führenden Rolle auf internationaler Ebene kann schwerlich bewertet werden, ohne dessen gleichzeitige Ambitionen im regionalen Umfeld zu betrachten. Die eigene Souveränität bzw. hegemoniale Stellung im Bereich des ›nahen Auslands‹ kann als eine Grundvoraussetzung für alle weiterführenden Status-Aspirationen gesehen werden: Nur über eine wirtschaftliche, politische, militärische, aber auch zunehmend kulturelle Kontrolle der ehemaligen Sowjetstaaten ist aus Putins Sicht die Stabilität Russlands nach innen und außen möglich. Auf militärischer Ebene spielt die Unterstützung nationaler Sezessionsbestrebungen in Ländern wie Georgien oder der Ukraine eine bedeutende Rolle, um auf Grundlage kulturell-ethnischer Legitimationsnarrative die Souveränität der Länder, zumeist infolge zunehmender West-Orientierung, in Frage zu stellen und faktisch zu untergraben. Dies geschah etwa durch die Vergabe russischer Pässe an BewohnerInnen der georgischen Regionen Abchasien und Ossetien (Delcour und Wolczuk 2015, S. 468). Durch diese Strategie wird aus russischer Sicht der Vorwurf entkräftet, die geforderte Nichteinmischung in die inneren Angelegenheiten anderer souveräner Staaten selbst missachtet zu haben. Wo kein souveräner Staat existiert, gibt es auch keine unrechtmäßige Intervention. Hiermit sind zwei konkrete Ziele verbunden: Erstens, die zunehmende Ost-Erweiterung der EU, vor allem aber der NATO zu unterbinden, was einen direkten Bezug zum beschriebenen Großmachtstreben darstellt, und zweitens, das Narrativ einer ›Russian World‹ zu propagieren, wonach im ex-sowjetischen Raum der russischen Nation zugehörige Menschen in ihnen kulturell fremden Rechtsräumen leben. Daher sei es Aufgabe Russlands, sie dort zumindest zu beschützen (Mankoff 2014, S. 64). Somit versucht das Regime, Interdependenzen der ideellen Ebene mit den BürgerInnen anderer Länder zu seinen Gunsten auszunutzen, diese noch weiter zu entfremden und im Idealfall einen gesteigerten Sezessionswunsch zu entfachen.[96] Auf diesen Aspekt der Präferenzkonstellation Putins und der Silowiki wird nachfolgend noch gesondert eingegangen.

An dieser Stelle sind dagegen zwei weitere Punkte im Rahmen russischer Regionalmachtsinteressen von besonderer Relevanz: Erstens die militärische Einhegung/

95 Nichtsdestotrotz legt bislang besonders die FSB-Gruppe Turla einen Schwerpunkt auf osteuropäische Regierungen, Ministerien und Botschaften als Ziele ihrer Spionage.

96 Inwiefern diese Strategie auf ideeller Ebene als erfolgreich gewertet werden kann, muss aufgrund von Umfragen in der Ukraine kritisch hinterfragt werden. Darin hatte sich eine große Mehrheit der BürgerInnen in Folge des russischen Vorgehens in ihrem Land zunehmend negativ über Russland und speziell Putin geäußert (Kuzio 2021).

Unterdrückung potenziell innerrussischer Sezessionsbestrebungen, zumeist als Anti-Terror-Kampf bezeichnet, zweitens das angestrebte Entfachen eines ›Rally-around-the-Flag‹-Effekts durch militärische Interventionen in Zeiten domestischer Unruhen. Im Falle der Ukraine-Krise konnten somit – neben den bereits beschriebenen Interessen des Kremls an der Verhinderung einer Verwestlichung der als Teil Russlands angesehenen Ukraine – noch weitere Ziele verfolgt werden. So stand das Regime in Folge der Präsidentschaftswahlen 2012 erheblich unter Druck, nicht jedem Russen oder jeder Russin gefiel der abermalige Positionstausch zwischen Putin und Medwedjew. Die Aktivierung patriotischer Gefühle gegenüber einem potenziellen ›Verlust‹ der ›Kiewer Rus‹ traf auf eine Interessenskompatibilität mit weiten Teilen der russischen Bevölkerung. So stiegen Putins Zustimmungsraten in Umfragen ab 2014 und fielen erst 2018 wieder etwas stärker (Levada 2021). Am deutlichsten wird dieser russische Ukraine-Konsens auch durch die Haltung des prominentesten Kritikers und Gegners Putins, Alexej Nawalny. Selbst für den hypothetischen Fall einer Präsidentschaft des ehemaligen Anti-Korruptionsgegners wird die bedingungslose Rückgabe der Krim an die Ukraine als unwahrscheinlich eingestuft, analog zu Nawalnys nationalistischen Äußerungen bezüglich des Georgienkrieges 2008 (Umland 2021).

Putin und die Silowiki sahen ferner die politische Stabilität des größten Flächenlandes der Erde in Folge der Tschetschenien-Kriege durch Sezessionsbestrebungen und auch durch islamistisch geprägten Terror gefährdet, besonders in der Kaukasus-Region mit ihrer geografischen Nähe zu Afghanistan.[97] Die militärische Präsenz in den russischen Regionen, aber auch den Nachfolgestaaten der UdSSR weiter auszubauen, stellte auch in Folge des elften Septembers 2001 einen zentralen Pfeiler der regionalen Sicherheitsarchitektur dar. Dabei kam es gewissermaßen zu einer russisch-chinesischen Arbeitsteilung im zentralasiatischen Raum: Russland als sicherheitspolitischer und China als wirtschaftlicher Akteur, eingebettet in den institutionellen Rahmen der SOZ. Hierbei erfolgte auch die Wiederaufnahme russischer Militärexporte nach China (Kaczmarski 2016). Im Zuge der sich abermals zuspitzenden Eskalation gegenüber der Ukraine trafen sich Putin und Xi im Februar 2022 in Peking und verfestigten ihre seit dem Beginn der Krise verstärkte Kooperation und Zusammenarbeit. Dies wurde u.a. dadurch erklärt, dass der Verlauf des Konfliktsund die Haltung des Westens auch einen Einfluss auf den Konflikt um Taiwan haben würden und umgekehrt, weshalb beide Länder an einer einheitlicheren Position gegenüber der NATO und besonders den USA interessiert seien (vgl. Maull 2022).

Die unterschiedlich gelagerten Interessen Putins und der Silowiki an einer hegemonialen Stellung Russlands in der Region haben somit ideelle, politische, militärische sowie wirtschaftliche Ursprünge und können als maßgeblich für die bereits genannten Cyberspionage-Operationen sowohl der Proxy-AkteurInnen als auch direktstaatlicher HackerInnen gegen unterschiedliche Ziele der Region gesehen werden. Die zahlreichen Spionage- und Sabotage-Operationen gegen die Ukraine, deren politische Institutionen,

---

97 »*Cases of Russian and central Asian citizens swelling the ranks of the terrorists have become more common. Many are now fighting in Syria. But they will represent the greatest threat when they return home.*« (Patrushev, in: Chernenko 2015).

kritische Infrastrukturen, Militärstreitkräfte, aber auch zivilgesellschaftliche AkteurInnen stehen exemplarisch für die Präferenz der umfassenden Unterminierung regionaler Gegner auf allen vier genannten Ebenen.[98] Ziel dabei ist es, entweder eigene Interdependenzvulnerabilitäten, etwa auf wirtschaftlicher Ebene, mithilfe von Cyberoperationen zu verringern (z.B. durch Spionage) oder die Verwundbarkeiten des Gegenübers und somit auch die hierbei bestehende Asymmetrie noch zu verstärken. Dem Kreml wurde etwa im Falle des Konflikts mit der Ukraineschnell bewusst, dass sich die westlichen Staaten offensichtlich nicht zu einer gemeinsamen Militärintervention zur Unterstützung des Landes würden durchringen können, auch nicht im Falle einer erneuten Eskalation im Jahr 2022. Somit konnte die eigene militärische Verwundbarkeit als geringer und die des Gegenübers als höher eingestuft werden, da Russlands Militärmacht gegenüber einer auf sich allein gestellten Ukraine deutlich überlegen wäre (Roth 2021). Die russischen Cyberoperationen im Rahmen des Krieges gegen die Ukraine hatten bislang in erster Linie einen substituierenden Charakter, es ging nicht darum, hierdurch entscheidende strategische Gewinne zu erzielen. Eine militärische Eskalation wurde in Kauf genommen, da die eigenen Verwundbarkeiten als geringer eingestuft wurden als die des Gegenübers. Dennoch folgte Russland mit seiner Strategie der asymmetrischen Kriegsführung auch in der Ukraine seiner verstärkten Neigung, Militärinterventionen zunehmend durch nicht militärische Konfliktaustragungsmittel, durchgeführt seitens unterschiedlicher, auch nichtstaatlicher AkteurInnen, zu komplettieren oder gar ganz zu ersetzen (Thornton 2017).[99]

Die beschriebenen Cyberoperationen gegen Stromversorgungseinrichtungen in der Ukraine 2015 und 2016 können nicht als ein russisches Mittel zur Veränderung der Asymmetrie gegenüber der Ukraine auf militärischem Terrain angesehen werden, sondern vielmehr als eine Art Signaling gegenüber Dritten, allen voran den USA. Die Botschaft konnte hier eigentlich nur sein, den russischen Willen und die Fähigkeiten zur Durchführung disruptiver Sabotage-Operationen unter Ausnutzung zuvor erlangter Zugriffsrechte auf kritische Infrastrukturen des politischen Gegners zu demonstrieren. Theoretisch gesprochen handelte es sich hierbei somit um den Versuch einer Manipulation

98 Ein weiteres Beispiel für den Versuch mithilfe von Cyberoperationen ›abtrünnige‹ Staaten der Region zu schwächen, bzw. mehr über deren weiterführende Intentionen in Erfahrung zu bringen und somit einer verstärkten Verwundbarkeitsasymmetrie auf militärischer Ebene in der Region entgegen zu wirken, ist der berichtete Malware-Einsatz seitens Fancy Bear gegenüber der montenegrinischen Regierung, in direktem zeitlichem Vorlauf zum offiziellen NATO-Beitritt des Landes (Dark Reading 2017).

99 Die sich im Januar/Februar 2022 und somit kurz vor der Abgabe dieser Arbeit andeutenden Kampfhandlungen in der Ukraine könnten jedoch nicht nur die Konfliktdynamik, sondern auch die Rolle von Cyberoperationen darin künftig verändern, d.h. weiter intensivieren oder aber ihre bloße Substitutionsrolle weiter festigen. Die im Januar 2022 berichteten Cyberoperationen mutmaßlich russischen Ursprungs gegen ukrainische Regierungswebseiten mit Hilfe von Defacements, aber auch Wiper-Operationen, zudem gepaart mit Desinformationskampagnen über deren Ursprung, fügen sich in das bisherige Operationsmuster russischer Proxies jedenfalls weitgehend ein (vgl. Biasini et al. 2022). Für den tatsächlichen Fall einer russischen Invasion erwarteten manche BeobachterInnen sogar eine gänzlich untergeordnete Rolle von Cyberoperationen gegenüber traditionellen Militärschlägen (Maschmeyer und Kostyuk 2022).

der Interdependenzasymmetrie gegenüber den USA: Sollten diese ihre eigenen Interessen weiterhin oder zunehmend zulasten russischer Ziele verfolgen, etwa in Syrien oder der Ukraine, müssten diese in der Zukunft mit ähnlichen Sabotage-Akten auf ihre eigenen Energieversorger rechnen, die durch Sandworm bereits seit 2011 infiltriert worden waren (Cloherty und Thomas 2014).[100] Die Attribution einer sich im weiteren Verlauf als GRU-Ableger entpuppenden Gruppierung konnte eine derart intendierte Bedrohungsperzeption auf amerikanischer Seite nur noch verstärkt haben.

Insgesamt spiegeln sich die in diesem Abschnitt aufgezeigten Interessen des Kremls an einer führenden Stellung Russlands in der Region in der Gesamtheit der verzeichneten Cyberoperationen besonders gegenüber osteuropäischen Ländern wider. Das breite Spektrum an hierbei eingesetzten Proxy-Gruppierungen, angeleitet durch verschiedene Geheimdienste, sowie die Vielfalt der dabei eingesetzten Methoden verdeutlichen den generellen Stellenwert dieser Präferenz. Wie im Falle der Ukraine besonders deutlich wurde, bestimmte das Konfliktpotenzial der domestischen Interessensdurchsetzung besagter Länder die Art und das Ausmaß russischer Cyberoperationen zur Manipulation der hierbei wahrgenommenen Verwundbarkeitsasymmetrien.

Russland als Zentrum einer ›*Russian World*‹

Als drittes Interesse Putins und der Silowiki wird nun die bereits erwähnte Proklamation einer ›Russian World‹ analysiert. Deren Fokus liegt auf ideell begründeten Legitimationsnarrativen, die durch sozio-kulturelle und ethnisch-linguistische Gemeinsamkeiten nationale Souveränitätsgrenzen ehemaliger Sowjetländer zu unterminieren versuchen. Dies hätte zudem auch auf politischer sowie wirtschaftlicher Ebene positive Nebeneffekte. Die beschriebene Selbstreklamation Putins der Verteidigung einer multiethnischen, russischen Gesellschaft sollte daher weniger als altruistisches denn strategisches Zukunftsprojekt interpretiert werden. Eine wichtige Rolle in diesem Zusammenhang spielte für Putin bislang auch der russisch-orthodoxe Geistliche Kyrill I. Diesem kam als dem Vorsteher der besagten Glaubensgemeinschaft bislang vor allem auch in anderen Ländern eine wichtige Integrationsfunktion gegenüber den dort beheimateten ethnischen RussInnen zu, sodass dessen Rolle von BeobachterInnen sogar mehr als die eines Politikers beschrieben wurde (Makarin 2019). Auch nach innen sprach er sich offen für Putin und dessen Regimeelite aus.

Dieses noch stärker auf der ideellen Ebene verortete Interesse Putins kann die verzeichneten Cyberoperationen russischer Proxys weniger direkt erklären, als das auf allen drei Liberalismus-Ebenen angesiedelte Interesse nach dem ethnisch-kulturell legitimierten Status einer Regionalmacht. Dennoch fügt es sich wie beschrieben darin ein, besonders in Bezug auf das russische Vorgehen in der Ukraine. Ein Beispiel für die wohl eher pragmatische Instrumentalisierung ethnisch-kultureller Narrative, um die als konfliktiv betrachtete Interessensdurchsetzung ehemaliger Sowjetgebiete auf dieser Ebene zu manipulieren, ist der sog. ›erste Cyberkrieg‹ der Geschichte: Die DDoS-Angriffe auf

100 Dass diese Botschaft in den USA durchaus vernommen wurde, zeigen auch die Warnungen des Department of Homeland Security (DHS) vor russischen Cyberoperationen im Falle einer US-Reaktion im Rahmen des Konflikts mit der Ukraine vom Januar 2022 (Barr und Margolin 2022).

Estland im Jahr 2007 erfolgten als direkte Reaktion auf die aus russischer Sicht ideologische Provokation Estlands der Entfernung einer sowjetischen Weltkriegsstatue in Tallinn. Die Interessen der in Estland beheimateten ethnischen RussInnen wurden somit zum Anlass genommen, um die Vorstellung einer ›Russian World‹ im nahen Ausland erstmals auch mithilfe disruptiver Cyberoperationen zu verfolgen. Russland wurde im Rahmen dieser Cyberangriffe eine eher indirektere Beteiligung im Sinne genereller Ermutigung und taktischer Unterstützung (›state-encouraged‹), z.B. durch das Bereitstellen von DDoS-Tools in Hackerforen, mithilfe der Jugendorganisation Nashi unterstellt (Pernik 2018, S. 57). Auch hier waren die Cyberoperationen wieder nur ein Teil einer multidimensionalen ›Coercion‹-Kampagne, die gegenüber einem benachbarten Land ebenfalls politische, ökonomische sowie diplomatische Zwangs- bzw. Druckmittel inkludierte (Pernik 2018, S. 57).

Die Interessen Putins und der Silowiki, die zu seinem innersten Kreis gehören und zumeist die führenden Posten in den zivilen und militärischen Geheimdiensteinheiten besetzen, bestimmten bislang primär Russlands Außenpolitik und somit auch die Cyberproxy-Nutzung. Dabei herrschte weitgehende Einigkeit in Bezug auf die ideellen sowie wirtschaftlichen Zielsetzungen: Russlands Position auf internationaler Ebene ist zu verbessern, indem in erster Linie das liberal-demokratische Lager um den US-Hegemon auch durch Cyberoperationen geschwächt wird, gleichzeitig ist Russlands Status als führende Regionalmacht im eurasischen Raum zu stärken, auch auf Grundlage eines instrumentalisierten ethno-kulturellen Legitimationsnarrativs. Politische Stabilität durch zentralisierte Staatsgewalt in den Händen weniger Personen im Umfeld Putins sowie deren Ämterbesetzung sowohl in der politischen Bürokratie als auch den zahlreichen Staatsunternehmen waren dabei die Hauptmaximen, um den eigenen exklusiven Herrschaftszugang nicht zu gefährden. Cyberproxys agierten gezielt gegen die genannten Bedrohungsperzeptionen (USA, liberal-demokratische Demokratie, EU/NATO-Osterweiterung). Hierbei sollten die eigenen Verwundbarkeiten in einem Anfang und Mitte der 2000er Jahre zunehmend liberal-demokratisch geprägten, internationalen Werteumfeld durch das Ausnutzen der Interdependenzvulnerabilitäten des Gegenübers im Cyberspace manipuliert werden.

Die republikanische Ebene spiegelt dabei einerseits wider, wie konzentriert der Herrschaftszugang im Kreml ist, andererseits, wie immer wieder ernstzunehmende Rivalitäten zwischen den AkteurInnen der Winning Coalition auftreten. Hieraus resultierten die beschriebenen parallel erfolgten Cyberoperationen sowie Diskreditierungen der jeweils anderen Geheimdienstbürokratien. Keiner der genannten AkteurInnen konnte für Putin bislang eine ernsthafte Gefahr darstellen, auch, da dieser den Wettkampf um seine Gunst stets erhielt und somit eine ›gesunde‹ Dauerrivalität förderte. Das Vorgehen gegen die FSB-Offiziere Anfang 2017, denen Geheimnisverrat an die USA vorgeworfen wurde, zeigt dabei, dass gegen potenzielle Fehltritte auch ranghoher Silowiki immer wieder energisch vorgegangen wurde, sofern deren Interessen denen des Regimes entgegenstanden. Andererseits kam es unter der Anleitung Putins auch zu

notwendigen Kooperationsansätzen zwischen FSB und GRU, wenn es die strategischen Präferenzen des Regimes erforderten (Cheravitch und Lilly 2020, S. 44).[101]

Für das Verhältnis des Kremls zu seinen durchaus international anerkannten und erfolgreichen IT-Unternehmen ist neben dem US-Boykott von Kaspersky-Produkten in der öffentlichen Verwaltung ab 2017 die Festnahme Ilya Sachkovs, des CEOs von IB-Group,[102] von Interesse: IB-Group hatte jahrelang u.a. mit Interpol zusammengearbeitet. Ende 2021 wurde gegen Sachkov der Vorwurf des Hochverrats erhoben, er habe Quellen zufolge Informationen über die Fancy Bear/GRU-Operationen im US-Wahlkampf 2016 an US-Behörden weitergegeben (Mitchell 2021). Sachkovs Fall scheint somit mit der Anklage der FSB-Offiziere 2017 im Zusammenhang zu stehen. Gleichzeitig verdeutlicht er, dass IT-Unternehmen mit Sitz in autokratischen Ländern stärker als in Demokratien zum Gegenstand staatlicher Kontrolle und Repressalien werden können, sofern deren Interessensdurchsetzung denen des Regimes widerspricht.

Entsprechend des russischen ›Power-Sharing‹-Mechanismus zwischen den Geheimdiensten, bei dem zwar lange der FSB im Cyberbereich die Oberhand hatte, in der Folge jedoch vor allem seitens des GRU in seiner Vorreiterrolle eingeholt wurde, teilten sich diese das breite Spektrum an erfassten Cyberoperationen mit russischer Verantwortungszuweisung. Historisch gewachsene Beziehungen, etwa zur organisierten Kriminalität, wie sie besonders dem FSB nachgesagt werden, hatten jedoch einen nachweislichen Einfluss auf die Ausgestaltung der Cyberproxy-Operationen im Sinne der AV II. Ein gewisser ›Cult of Secrecy‹ der unter Putin in zentralen Positionen befindlichen Ex-KGB-AkteurInnen beförderte besonders in den 2000er Jahren eine prinzipielle Neigung der Behörden, Informationen oftmals nicht mit anderen staatlichen Entitäten zu teilen (Peterson 2005, S. 59). Somit sprach besonders in den Anfangsjahren des Cyberkonfliktaustrags viel für die Beauftragung von Dritten außerhalb des politischen Systems. Die seitens des FSB orchestrierten Yahoo-Hacks verdeutlichen jedoch, dass auf nationaler Ebene brisante Spionage-Operationen auch im weiteren Verlauf immer wieder an solche Drittakteure ausgelagert wurden. Da die notwendigen Druck- und Kontrollmittel verfügbar waren, konnten ihre Handlungen komplementär zu den eigenen Interessen gehalten werden. Die Verhaftung russischer Cyberkriminelle im Januar 2022 deutet jedoch eine Verschiebung der Beziehung zwischen Staat und Proxys zumindest an.

Deutlich wurde außerdem, dass zwar alle drei Geheimdienste, FSB, GRU und SWR, im Laufe der Jahre immer stärker eigene Kapazitäten im Cyberspace entwickelten, das Ausweichen auf tatsächliche Proxys jedoch nach wie vor in ihrem jeweiligen Interesse liegt. Verantwortlich hierfür sind ihre bloße Verfügbarkeit sowie die oftmals damit angestrebte ›Plausible Deniability‹. An dieser Stelle kann jedoch nicht beurteilt werden, ob der Proxy-Gebrauch eine von Putin selbst regelmäßig vorgegebene Handlungsmaxime ist oder ob die Geheimdienste diese historisch gewachsene Praxis regelmäßig auch auf den Cyberspace übertragen.

101 So kam es 2017 zu einer Art Abkommen zwischen den beiden Geheimdiensten, in welchem der FSB dem GRU seine Unterstützung bei der Ausbildung von KryptographInnen zusagte.

102 IB-Group ist das zweite IT-Unternehmen aus Russland, das als Attributionsquelle im HD-CY.CON verzeichnet wurde.

Ein weiteres interessantes Merkmal russischer Cyberoperationen, gerade in Bezug auf die IV, ist das Bestreben der Geheimdienste und somit auch der Silowiki, durch Cyberoperationen regelmäßig negative Konsequenzen ihrer konventionellen Handlungen reduzieren zu wollen. Dies geschah während des versuchten Hacks der Organisation for the Prohibition of Chemical Weapons (OPCW) 2018, um deren Untersuchung zur Vergiftung des Ex-GRU-Agenten Sergej Skripal überwachen, wenn nicht gar sabotieren zu können. Zudem hatten die gleichen Hacker vermutlich ähnliche Operationen gegen die Untersuchungen zum Abschuss der MH17-Maschine in der Ukraine 2014 geplant, der ebenfalls mit dem analogen Arm des GRU in Verbindung gebracht wurde (Deutsche Welle 2018; Rakuszitzky et al. 2018). Der militärische Hintergrund des GRU konditionierte somit in erheblicher Hinsicht dessen Angriffsprofil, insbesondere im Rahmen gewaltsamer Konflikte wie dem Ukraine-Konflikt. Die aufgezeigten Entwicklungen haben gezeigt, dass der GRU in Nachgang des Georgienkrieges in der Lage war, nicht nur auf eine gewaltsame ›Lösung‹ des Ukraine-Konflikts durch die Annexion der Krim zu drängen, sondern mithilfe seiner Hacker-Gruppierungen Fancy Bear und Sandworm den hiermit verbundenen, wenn auch stets offiziell bestrittenen russisch-ukrainischen Krieg auch im Cyberspace zu unterstützen. Der GRU festigte somit seinen während gewaltsamen Konflikten vergrößerten Herrschaftszugang. Darüber hinaus expandierte er stetig seine Tendenz zur Information-Warfare (Weiss 2020), die daher auch in Friedenszeiten gegenüber demokratischen Zielen wie den USA und Frankreich zunehmend Anwendung fand (Troianovski und Nakashima 2018).

5.4.3.3 Weitere Akteure des ›Inner Circle‹: Liberale und Technokraten

In Opposition zu den Silowiki werden in der Literatur vereinzelt die sog. ›Liberalen‹ sowie ›Technokraten‹ des inneren Zirkels um Putin dargestellt. Zu diesen zählten Anwälte oder Ökonomen wie der frühere Finanzminister Alexei Kudrin, German Gref als früherer Wirtschaftsminister und besonders Dmitri Medwedew, der sich wiederholt mit Putin in der Rolle des Präsidenten und Ministerpräsidenten abwechselte. Diesen wird verstärkt in den frühen 2000er Jahren ein neoliberaler Einfluss auf die russische Wirtschaft attestiert. Die von ihnen angestrebten Marktreformen sowie Streitigkeiten bezüglich Budgetfragen führten zu einer zeitweiligen Opposition zu den Silowiki und nationalistischen Abgeordneten in der Duma (Rutland 2018, S. 284).

Als Medwedew 2008 zum russischen Präsidenten gewählt wurde, waren sich BeobachterInnen uneinig, inwiefern er eigene Politikakzente setzen oder lediglich Putins Anweisungen Folge leisten würde. In einer Rede im Januar 2008, damals noch als Präsidentschaftskandidat, betonte Medwedew seinen Fokus auf die wirtschaftliche Weiterentwicklung Russlands sowie dessen natürliches Interesse an engen Beziehungen zum Raum der Gemeinschaft unabhängiger Staaten (GUS), zwei Standpunkte, mit denen Putin weitgehend übereinstimmte. Zusätzlich betonte er jedoch auch die Bedeutung »*einflussreicher und unabhängiger Medien*«, um einen »*freien Informationsfluss*« zu gewähren, sowie die notwendige Hinwendung des Landes zu rechtstaatlichen Strukturen: »*Leider kann sich kein anderes europäisches Land mit einem solchen Ausmaß von Rechts-Missachtung rühmen*« (zitiert in: Deutsche Welle 2008b). Diese zwei Positionen deuteten schon stärker ein in Teilen von Putins Diktum abweichendes politisches Programm an. Seinen Worten Taten folgen ließ Medwedew zumindest in Bezug auf die Unabhängigkeit der Medien im De-

zember 2009, als er ein von Putin initiiertes, verschärftes Mediengesetz mit seinem Veto zum Scheitern brachte.

Die im selben Zeitraum zum Ausdruck gebrachte Intention des neuen Präsidenten, Russland zu einem umweltfreundlicheren Staat zu machen, reflektierte ebenfalls dessen stärker liberalere Gesinnung im Gegensatz zu Putin und den Silowiki (Tagesschau 2009). Ebenso ging Medwedew im Militärbereich gegen dort weitverbreitete Korruptionspraktiken zu Beginn seiner Amtszeit vor, indem er auf Betreiben des Verteidigungsministers Serdjukow den Generalstabchef der Armee absetzte, um Reformen in der russischen Armee vorantreiben zu können. Letzteres schien jedoch auch dem damaligen Interesse Putins an einer stärkeren Kontrolle des Kremls über die Streitkräfte zu entsprechen, weshalb er selbst Serdjukow 2007 erst zum Verteidigungsminister ernannt hatte (Wipperfürth 2011, S. 104).

Insgesamt wird Medwedews Präsidentschaftszeit zumeist zweigeteilt bewertet: Während er seine liberaleren und damit Putins Haltungen oftmals widersprechenden Positionen auf der domestischen Ebene verfolgte, stand seine sicherheitspolitische Außenpolitik stärker im Einklang mit Putin. Beispiele für Medwedews innerstaatliche Reformbemühungen sind die merkliche Liberalisierung der Mediengesetze, eine zumindest in Ansätzen eingeleitete Reform des nationalen Justiz- und Gefängnissystems, die Wiedereinführung größerer Entscheidungsfreiräume der Oligarchen sowie größere Diskursanteile für WissenschaftlerInnen und Intellektuelle, etwa im Rahmen des 2008 gegründeten *»Instituts für Moderne Entwicklung«* (Lebahn 2010).

Im Gegensatz dazu entwickelte sich das russisch-westliche Verhältnis während der Präsidentschaft Medwedews in einer Art ›Schlingerkurs‹: Eine erste Zerreißprobe war das russische Vorgehen während des Georgienkonfliktes 2008. Dabei kam es zu einer scheinbaren Abkehr des russischen Dogmas der Unversehrtheit nationaler Souveränitäten zu Gunsten des laut russischer Argumentation unterdrückten Selbstbestimmungsrechts der Abchasen und Osseten sowie sich einem gegenüber diesen Gruppierungen abzeichnenden Genozid (Wipperfürth 2011, S. 104). Der unter Medwedew geleitete Militärfeldzug (und somit auch die im unmittelbaren Vorfeld stattgefundenen Cyberoperationen) stand somit im Widerspruch zu den in der Folge angestrebten Bemühungen des Präsidenten, enge wirtschaftliche Beziehungen nicht nur zum ›nahen Ausland‹, sondern im Rahmen einer angestrebten ›Modernisierungspartnerschaft‹ auch zu europäischen Ländern aufzubauen. Dies deutet daraufhin, dass Medwedews Präferenzen auf der ideellen Ebene denen Putins und der Silowiki in Bezug auf das Interesse an einer russischen Vormachtstellung in der Region eher entsprachen als auf der ökonomischen Ebene, sich diese Zielsetzungen dadurch jedoch zeitweilig behinderten und im Zweifel die ideell-sicherheitspolitischen Interessen präferiert wurden.

Nachdem besonders die USA eine konsequente Reaktion auf Russlands Georgienintervention vermieden hatten, kam es im Rahmen der Ämterwechsel Putin-Medwedew und Bush-Obama durch die Unterzeichnung des ›New START‹-Abrüstungsvertrages 2010 zur Andeutung des sog. ›Reset‹. Auch eine mögliche NATO-Mitgliedschaft des Landes wurde weitaus offener diskutiert, was im Gegensatz zur politisch angespannten Atmosphäre nach Putins Rede auf der Münchner Sicherheitskonferenz 2007 stand (Krumm 2010, S. 11). Nichtsdestotrotz führte die Thematik der europäischen Sicherheits- und Verteidigungsarchitektur, z.B. die zeitweilig geplanten Raketenab-

wehrsysteme in Polen und Tschechien, immer wieder zu Spannungen zwischen den osteuropäischen Ländern und den NATO-Verbündeten, aber auch zwischen ihnen und Russland. Insgesamt wurde das russisch-westliche Verhältnis zwischen 2009 und 2011 jedoch als wesentlich kooperationsgeprägter bewertet als zuvor und danach. Der Kurs der wirtschaftlichen Modernisierung und zeitweiligen Konzessionsbereitschaft gegenüber westlichen Ländern wurde von Putin vermutlich auch mitgetragen, weil die Finanzkrise 2008 Russland getroffen hatte, worunter der Ölpreis und somit auch die russische Wirtschaft und die russischen BürgerInnen leiden mussten.

Wie bereits angedeutet, verhielten sich Medwedews Präferenzen auf wirtschaftlicher sowie republikanischer Ebene (etwa durch angestrebte institutionelle Reformen im Zuge der vor allem aus wirtschaftlicher Sicht notwendigen Korruptionsbekämpfung) in Teilen konfliktiver zu den Silowiki als die des Präsidenten Putins. Festhalten lässt sich jedoch, dass es zwar zu Ämterrochaden in Geheimdienstbehörden wie der Einsetzung des Medwedew-Vertrauten Bortnikov als FSB-Chef kam, aber z.B. genau diese Behörde in der Folge auch mithilfe erlassener Gesetze ihre genuine Einflusssphäre auf die innerrussischen Geschicke sogar noch ausweiten konnte. Dies war auch aufgrund proklamierter Kompetenzerweiterungen des Geheimdienstes im Zuge der Terror-Bekämpfung nach 9/11 möglich, die auch Medwedews Präferenzordnung entsprach (Singhofen 2010, S. 208).

Insgesamt lässt sich Medwedews Herrschaftszugang während seiner Präsidentschaft im Vergleich zu seiner Zeit als Ministerpräsident naturgemäß als größer bezeichnen. Dabei setzte er seine Interessen vor allem im wirtschaftlichen Bereich nach innen und außen durch und positionierte sich damit in zeitweiliger Opposition zu Putin und den Silowiki. Das gesamte Machtgefüge wird während der Jahre 2008–2012 von BeobachterInnen nichtsdestotrotz als das eines Tandems, bestehend aus Medwedew und Putin, bezeichnet, das konkurrierende Machtgruppierungen innerhalb des Kremls ausbalancierte und somit die Stabilität des Systems gewährleistete. Dass Medwedew in seiner Amtszeit Putins Interessensdurchsetzung wohl nicht allzu sehr eingeschränkt hatte, zeigt letztlich auch dessen Berufung als Putins Nachfolger im Ministerpräsidentenamt ab 2012.

Bezüglich Medwedews Einfluss auf die russischen Cyberproxy-Operationen lassen sich folgende Aussagen treffen: Die im Zeitraum von 2008 bis 2012 gestarteten Cyberoperationen lassen auf keinen spezifischen Funktionsschwerpunkt schließen. Auch die daran beteiligten Hackergruppierungen lassen sich allen drei genannten Geheimdiensten zuordnen. Die Cyberoperationen während des Georgienfeldzuges markierten eine Art Testlauf für die Integration russischer Cyberkapazitäten im Rahmen gewaltsamer Konflikte, die Jahre später im Rahmen des Ukraine-Feldzuges weiter intensiviert werden sollte und die dominante Rolle des GRU während gewaltsamer Konflikte auch im Cyberspace begründete. Somit ist zwar von einem Einfluss Medwedews auf manche Ämterbesetzungen der Geheimdienste wie im Falle Bortnikovs auszugehen. Die insbesondere seitens des GRU zunehmend disruptiven Operationen entsprachen jedoch nach wie vor der Interessensdurchsetzung der Silowiki auf ideell-nationalistischer Ebene. Begünstigend wirkte hierbei die Interessenskompatibilität zwischen Silowiki und Medwedew im Hinblick auf das russische Vorgehen im Georgienkonflikt.

Zwei konkrete Cyberoperationen sollen an dieser Stelle explizit diskutiert werden. Begonnen wird mit der ersten im Datensatz verzeichneten Spionageoperation Sandworms, die von 2009–2014 andauerte und Länder wie die USA, Polen, Ukraine und die Slowakei, aber auch die NATO in einer Reihe von Sektoren (politische/staatliche Behörden, kritische Infrastrukturen, Zivilgesellschaft) anvisierte (Zetter 2014). Der regionale Fokus spiegelt das von Medwedew verfolgte Ziel der wirtschaftlichen Modernisierung Russlands, auch durch den Aufbau intensivierter Beziehungen zu besagten Ländern, wider. Das Abgreifen interner Informationen und Daten konnte für ein solches Vorhaben nur von Vorteil sein, etwa in privatwirtschaftlichen oder politischen Verhandlungen auf ökonomischer Ebene. Gleichzeitig verdeutlicht die Kampagne die Kontinuität russischer Cyberspionageoperationen gegenüber osteuropäischen Staaten, sei es mit einem stärker sicherheitspolitischen oder wirtschaftspolitischen Fokus.

Zweitens stellte die Hack-and-Leak-Operation der ›Climategate-Mails‹ Ende 2009 die erste im Datensatz verzeichnete russische Doxing-Operation dar und könnte Ausdruck der unter Medwedew oftmals autonomen Interessensdurchsetzung russischer Geheimdienste im Cyberspace sein. Im Vorfeld der UN-Klimakonferenz im 2009 hatten russische Hacker interne E-Mails und Dokumente der Universität von East Anglia gehackt und veröffentlicht. Darin wurde der Forschungsstrang zur Erderwärmung in ein negatives Licht gerückt bzw. die offensichtlich strategische Nichtveröffentlichung diverser Studien offengelegt (Stewart 2009), ein Beispiel des ›Liberal Mimicry‹, bereits sieben Jahre vor dem DNC-Hack. Der Hack könnte somit Ausdruck der Interessensinkompatibilität zwischen Geheimdiensten und Medwedew sein, der infolge der Krise 2009 einen größeren Schwerpunkt auf umweltfreundlichere Wirtschaftspraktiken legte (Henry und Sundstrom 2012).

5.5 Chinesische und russische Cyberproxy-Nutzung im Vergleich

> »Every external operation is first and foremost a domestic one: the single most important role of the agencies is to secure the regime.«
>
> *Mark Galeotti über russische Geheimdienstoperationen (2016b, S. 8)*

Auch wenn sich das Zitat von Mark Galeotti auf die russischen Geheimdienste bezieht, beschreibt es ebenso das Hauptmotiv der durch die PLA und das MSS angeleiteten chinesischen Cyberproxys. Wie die liberale Analyse der dabei zugrunde liegenden Interessen und Präferenzordnungen aufzeigte, kam es jedoch zu unterschiedlichen Cyberproxynutzungsmustern zwischen den zwei Autokratien.

Grundlegend können für China und Russland die aufgestellten Hypothesen der Wirkweise der UV weitgehend bestätigt werden. Um die eigene Verwundbarkeit gegenüber dem Ausbleiben technologischer Entwicklung zu reduzieren und somit die eigenen ideellen und kommerziellen Interessen verfolgen zu können, wendet die VR bislang in erheblichem Maße Cyberproxy-Operationen mit dem Ziel der Spionage

gegen demokratische Innovationsführer an. Der HD-CY.CON spiegelt die aufgezeigte Interessensbildung der KPC unter Hu Jintao sowie Xi Jinping nach einer nachhaltigeren Wirtschaftsentwicklung wider, um das hohe Maß an Korruption innerhalb der Partei nicht zu einer Gefahr für sich selbst werden zu lassen. Eine von manchen Wirtschaftsentrepreneuren geforderte Demokratisierung der KPC entsprach bislang nicht dem Parteiinteresse nach exklusivem Herrschaftszugang im politischen System, wodurch sich die repressiven Maßnahmen gegen international erfolgreiche Technologieunternehmen zumindest in Teilen erklären lassen. Das KPC-Interesse nach einer veränderten Interdependenzasymmetrie auf wirtschaftlicher sowie technologischer Ebene, insbesondere gegenüber den USA als Marktführer, kann somit für die UV sowohl H1, H2 als auch H3 hinsichtlich der im HD-CY.CON verzeichneten Cyberoperationen größtenteils plausibilisieren.[103] Das liberal-kapitalistische Wirtschaftsmodell demokratischer Länder führte zwar zu deren Führerschaft in wesentlichen Schlüsselindustrien, hinterließ diese jedoch aufgrund eines gleichzeitig niedrigen Niveaus an staatlicher Kontrolle und Einflussnahme zunehmend verwundbar gegenüber ausländischen Beeinflussungsmaßnahmen. Hinzu kommt, dass das staatlich subventionierte Wirtschaftsmodell Chinas immer stärker mit dem kapitalistischen System demokratischer Länder in Konflikt geriet. Dies betrifft nicht nur die beschriebenen FDIs chinesischer Unternehmen, sondern auch das hohe Maß an kommerziell motivierter Cyberspionage gegenüber demokratischen Ländern, was als effektivstes Mittel zur Manipulation der Interdependenzasymmetrien angesehen wurde.

Auch auf regionaler Ebene lassen sich besonders H1 und H3 der UV für China bestätigen: Die Rolle südostasiatischer Länder im regionalen Handelsgefüge, aber auch deren außen- und sicherheitspolitische Präferenzen gestalteten sich besonders unter Xi immer konfliktiver zu den Präferenzen der KPC im Hinblick auf territoriale Souveränitätsansprüche im südostasiatischen Raum. Um somit die politischen, aber auch militärischen Verwundbarkeiten gegenüber diesen oftmals mit den USA verbündeten Regionalstaaten zu reduzieren, wurden verstärkt Cyberproxys zur Schaffung von Informationsasymmetrien eingesetzt, mit Implikationen für die politische, militärische sowie ökonomische Ebene. Auch die berichteten Cyberoperationen gegenüber den ›Five Poisons‹ und somit aus chinesischer Sicht ausnahmslos domestischen AkteurInnen können durch die wahrgenommene Verwundbarkeit der KPC auf ideeller Ebene erklärt werden. Gleiches gilt für den Nutzen, der einer umfassenden Überwachung politischer GegnerInnen in Form von Cyberspionage seitens der KPC beigemessen wird.

Die H2 der UV entwickelt für die regionalen Spannungen um den Pazifikraum erst im Verbund mit der Rolle der USA eine ausreichende Erklärungskraft. So hat wohl deren

103 *H1 (UV):* Je größer die eigene Verwundbarkeit im Rahmen konfliktiver Präferenzinkompatibilitäten zu anderen Staaten auf einer oder allen drei Liberalismus-Ebenen ist, desto größer sind die autokratischen Anreize für die Nutzung offensiver Cyberproxys.
H2 (UV): Je stärker aufgrund konfliktiver Präferenzkonstellationen Regimetypenunterschiede in asymmetrischen Verwundbarkeiten resultieren, desto stärker sind die autokratischen Anreize für eine offensive Cyberproxy-Nutzung dem jeweiligen Staat gegenüber.
H3 (UV): Je größer der erwartete Nutzen bestimmter Formen offensiver Cyberproxy-Operationen zur Reduzierung eigener Verwundbarkeiten auf ideeller und/oder wirtschaftlicher Ebene ist, desto wahrscheinlicher ist deren Anwendung seitens der jeweiligen Autokratie.

›Pivot to Asia‹ in Teilen dem chinesischen Interesse nach militärischer Dominanz in der Region entgegengestanden, was einen Großteil der politisch-militärischen Cyberspionage gegen die USA, Japan sowie verschiedene ASEAN-Staaten erklären kann.

Die Abwesenheit disruptiver Cyberoperationen im Rahmen gewaltsamer HIIK-Konflikte sowie der Umstand, dass für die darin stattgefundenen Cyberspionageoperationen MSS-AkteurInnen verantwortlich gemacht wurden, spricht bei China gegen die Erklärungskraft der IV-Hypothesen in ihrer jetzigen Form: So wird gerade im Vergleich zu Russland angenommen, dass das relativ niedrige HIIK-Intensitätsniveau dieser gewaltsamen Konflikte (max. 3 von 5) gegenüber hauptsächlich domestisch geprägten AkteurInnen wie Hongkong oder Tibet, aber auch den Konfliktparteien um das Südchinesische Meer, die Anreize für einen disruptiveren und somit notwendigerweise seitens militärischer AkteurInnen geführten Einsatz von Cyberoperationen mit physischen Effekten für das Regime minderte. Ein Konflikt, der z.B. wie im Falle Russland mit der Ukraine bereits entsprechend der HIIK-Skala zu einem Krieg eskaliert ist, bedarf nicht mehr der gleichen Zurückhaltung gegenüber disruptiven Cyberoperationen, weshalb die H1 der IV für Russland auch weitgehend bestätigt wird.[104] Die prominente Rolle des GRU-Ablegers Sandworm bei der Durchführung der Stromausfälle in der Ukraine indizieren ferner eine hohe Erklärungskraft der H2 der IV für Russland,[105] gleiches gilt für die beschriebene Fancy-Bear-Operation mithilfe einer manipulierten App für die ukrainischen Streitkräfte. Gleichzeitig legen die berichteten Infiltrationen westlicher Energienetzwerke und Betreiber kritischer Infrastrukturen jedoch eine mögliche Eskalationssteigerung Russlands nahe, auch in offiziellen Friedenszeiten zumindest vorbereitende Maßnahmen für später vielleicht einmal notwendige Sabotageakte zu treffen. Interessant wird in diesem Zusammenhang für die Zukunft sein, wann Staaten wie die USA Cyberkriminelle wie die Ransomware-Gruppierung DarkSide konsequent als durch Russland geduldet und somit gewissermaßen auch unterstützt attribuieren. Dies würde bedeuten, dass deren disruptive Operationen gegenüber Betreibern kritischer Infrastrukturen wie Colonial Pipeline im Mai 2021 als russischer Sabotageakt gewertet und somit durch mögliche Gegenmaßnahmen sanktioniert werden könnten, trotz fehlendem gewaltsamen Konflikt als Eskalationsgrundlage.

Der Blick auf 2020 und 2021 legt jedoch auch für China eine zunehmende Integration von disruptiven Cyber- und traditionellen Militäroperationen nahe, wie am Beispiel des Konfliktes mit Indien im Himalaya-Gebirge und dem kolportierten Stromausfall in Mumbai aufgezeigt wurde. Ob dabei die PLA durch das SSF die Hoheit im Cyberspace innehat oder haben wird, kann an dieser Stelle nicht beurteilt werden. Eine stärkere Abstimmung und Koordination zwischen PLA und MSS wurde zumindest in einem Fall technologischer Spionage gegen ein britisches Unternehmen angedeutet und könnte auf eine eingeschränktere Erklärungskraft der zweiten Hypothese über das Wirken der IV

104 *H1 (IV):* Je gewaltsamer das bestehende allgemeine Konfliktniveau ist, desto wahrscheinlicher ist auch ein intensiverer/disruptiverer Einsatz autokratischer Cyberproxys, etwa gegen kritische Infrastrukturen des Gegners.

105 *H2 (IV):* Je stärker die angewandten Cyberoperationen Verwundbarkeitsasymmetrien im Rahmen militärischer Konflikte manipulieren sollen, desto eher ist von einer militärischen Kontrolle autokratischer Cyberproxys auszugehen.

für China zumindest hindeuten. Die Ergebnisse der IV-Hypothesen für China bekräftigen jedoch in gewisser Weise zusätzlich das Wirken der H3 der UV: Für China konnten disruptive Cyberoperationen gegen Ziele auf dem eigenen Staatsterritorium, etwa gegen Tibet oder die Uiguren in Xinjiang, vermutlich auch deshalb kein geeignetes Mittel sein, da dies noch stärker ungewollte Kollateralschäden für das chinesische Kernland hätte haben können, im Gegensatz zur russischen Sabotage in der Ukraine.

Auf russischer Seite bestätigen ebenfalls sowohl die Häufigkeit als auch das konkrete Profil der liberal-demokratischen Länder unter den Zielen der attribuierten Cyberoperationen die ersten beiden Hypothesen über das Wirken der UV. Die dabei stetig inkompatiblere Präferenzkonstellation auf ideeller Ebene, bedingt vor allem durch das liberal-demokratische Selbstverständnis, machte Länder wie die USA zu immer attraktiveren Zielen für russische Cyberoperationen. Neben dem ideellen ›Autokratie-vs.-Demokratie‹-Konflikt können besonders regionalpolitische Interessen Putins, der Silowiki und Medwedews die zahlreichen Operationen gegenüber den hierbei potenziell in Opposition stehenden Ländern und AkteurInnen erklären; sei es im Rahmen der angestrebten Verhinderung der NATO-Osterweiterung, vor allem gegenüber der Ukraine, oder im Kontext ideell-nationalistischer Konflikte mit einzelnen Staaten des Baltikums, etwa Estland, in denen die Interessen der dort angesiedelten ethnischen RussInnen gewusst amplifiziert und durch disruptive Cyberoperationen unterstützt wurden.

Hinzu kommt das Operationsprofil der russischen AngreiferInnen: Die verwendeten Maßnahmen, mal verdeckt wie im Falle politischer Spionage, mal bewusst offen wie bei den beschriebenen Doxing-Operationen, sind stets an die jeweils zu manipulierende Interdependenzvulnerabilität angepasst. Der Cyberspace bietet zwar umfassende Möglichkeiten für AkteurInnen, die gezielt unentdeckt und anonym handeln wollen, jedoch auch für solche, die ebenfalls ein hinreichendes Maß an Anonymität zur plausiblen Abstreitbarkeit anstreben, ihre Handlungen jedoch bewusst öffentlich gestalten *müssen*, um ihre Ziele zu erreichen.[106] Dies war vor allem für die russischen Doxing-Operationen, aber auch die beschriebenen Sabotage-Akte gegenüber ukrainischen Zielen der Fall. Wann immer das Ziel ist, Informationen des Gegenübers zu erhalten, ohne dass dieser davon Kenntnis hat, ist Cyberspionage das Mittel der Wahl und wurde aufgrund der aufgezeigten geostrategischen Interessen Russlands gegenüber den USA sowie osteuropäischen Ländern in zahlreichen Fällen angewandt. Wenn es jedoch eher um sog. ›Perception-Hacks‹ ging,[107] wurden Doxing sowie Sabotageakte zur Demonstration der eigenen Fähigkeiten als erfolgversprechender angesehen.

Diese Zusammenhänge verdeutlichen die Plausibilität der autokratischen H3 der UV für Russland, wobei jedoch einschränkend festgehalten werden muss, dass diese Annahmen (wie für China auch) auf der Grundlage einer Art Ex-post-Motivations- sowie -Verantwortungszuschreibung und teilweise aus der primären Perspektive der westlichen

---

106 Die unterschiedliche Verwendung verdeckter vs. offener Interventionsversuche in nationale Wahlen wird beispielsweise in Levin 2020 beschrieben. Für Staaten wie Russland kann eine nur scheinbare ›deniability‹ sogar gewollt sein, um die Gegenüber wissen zu lassen, dass man selbst für die Cyberoperation verantwortlich war und trotzdem straffrei davonkommen kann.

107 Diese werden verstanden als »[…] *an attempt to weaponize uncertainty to sow distrust and division*« (Nathaniel Gleicher, zitiert in: Myre 2020).

Öffentlichkeit erfolgt sind. Nichtsdestotrotz wurde deren Plausibilität auf Grundlage der unabhängig hiervon analysierten autokratischen Präferenzen verständlich gemacht.

Zuletzt gilt es die Aussagekraft der H4 für die UV zu bewerten:[108] Der für China festgestellte Wandel der Zuständigkeiten im Cyberspace ab 2015 zeigt auf, dass speziell unter Xi der Aktivitätsradius der PLA-HackerInnen stärker auf militärische Operationen kanalisiert wurde und somit deren unter Hu noch weitaus prävalentere Cyberspionageoperationen stärker dem MSS zufallen. Unter Hu verfügte die PLA über einen stärkeren Herrschaftszugang und konnte auch im Cyberspace freier agieren, brachte jedoch gleichzeitig durch ihre teilweise defizitäre Operational Security die Interessensdurchsetzung der KPC auf wirtschaftlicher Ebene zeitweise in Gefahr (s. die US-Sanktionen 2014 sowie damit einhergehend das Obama-Xi-Agreement 2015). Die PLA-Umstrukturierung unter Xi kann somit als Versuch gewertet werden, das Militär einerseits auch im Cyberspace zu modernisieren und auf potenzielle Militäroperationen vorzubereiten, andererseits jedoch die nach wie vor mit hoher Bedeutung versehenen Cyberspionageoperationen durch subtiler und technisch oft versierter agierende MSS-AkteurInnen wieder mit größerer Plausible Deniability durchführen zu können. Unter Xi fand eine noch stärkere Zentrierung und Personalisierung des Herrschaftszugangs statt, worin er sowohl die KPC-Eliten als auch die Militär- und GeheimdienstakteurInnen umfassend unter seine Kontrolle brachte und von sich abhängig machte. Die berichteten Coup-Pläne legen jedoch nahe, dass Xis Politik innerhalb der Winning Coalition nicht nur auf Zustimmung stößt, weshalb es für die Zukunft interessant sein könnte, inwiefern er an diesen internen Bedrohungsperzeptionen auch das chinesische Cyberkonfliktmanagement ausrichtet.

Bezüglich der Inkorporierung kommerzieller bzw. krimineller AkteurInnen als Cyberproxys kann eine gegenläufige Entwicklung innerhalb der beiden Länder resümiert werden: Während in China durch das MSS im Laufe der Zeit zunehmend IT-Unternehmen zu Gehilfen des Staates wurden und dabei jedoch auch eigenmotivierte kriminelle Aktivitäten entfalteten, entwickelten sich Russlands kriminelle Proxys offenbar (in Teilen) von Cyberkriminellen mit ad hoc-Beziehungen zum Staat zu kommerziellen, professionell anmutenden *Cybercrime*-Unternehmen.

Für Russland verdeutlicht die beschriebene Heterarchie zwischen verschiedenen Geheimdienstbehörden das bewusste Ausbalancieren der AkteurInnen und ihrer Interessen untereinander, wobei Putin zwar nicht für alle Cyberoperationen direkt verantwortlich ist, ihm jedoch die Möglichkeit und der Wille zu notwendigen Korrekturen attestiert werden können. Die informelle, über persönliche Kanäle erfolgende Interessenvermittlung und zentralisierte Repräsentation auf politischer Ebene werden durch die beschriebenen Geheimdienstkonflikte und -interaktionen sowie deren jeweilige Initiativen zur

108 *H4 (UV):* Je größer die domestischen Verwundbarkeiten autokratischer Regierungen auf republikanischer Ebene aufgrund inkompatibler Präferenzkonstellationen sind, desto eher ist die Auswahl und institutionelle Anbindung der Proxys auch auf deren Manipulation ausgerichtet.

Verbesserung der eigenen Stellung im institutionellen System widergespiegelt.[109] Der auf das Demonstrieren von Stärke und personalisierter Führung ausgerichtete Legitimationsansatz Putins kann offensichtlich auch auf das interne Legitimationsbestreben der Geheimdienste übertragen werden sowie auf deren Automatismus, im Falle fehlender Performanz (z.B. GRU im Georgienkrieg) in der Folge noch aggressiver vorzugehen, um somit die eigenen Legitimationseinbußen wieder zu kompensieren. Auch das kolportierte Verhältnis von FSB und GRU zu Cyberkriminellen und patriotischen HackerInnen sowie die sowohl auf Druck als auch auf positiven Anreizen basierende Beziehung zwischen den Seiten fügen sich in dieses Bild auf republikanischer Ebene ein. Politische Seilschaften und Interessenskonvergenzen waren dabei maßgeblicher für Ämterbesetzungen und inhaltliche Entscheidungen als formalisierte und standardisierte Prozesse. Die Art der Beziehung zwischen Auftraggeber und Stellvertreter kann als eine Mischung aus strafrechtlicher Bedrohungskulisse und in Teilen patriotischer Anstiftung beschrieben werden, mit voraussichtlich größeren Anteilen Ersterer im Falle von profit-orientierten Kriminellen. Patriotische Hacker wie das Kollektiv CyberBerkut folgen dagegen Akteuren wie Fancy Bear offensichtlich stärker aus ideologischer Gesinnung und operieren ebenfalls nicht notwendigerweise vom russischen Staatsterritorium aus.

Offen blieb jedoch bislang, ob auch im Cyberspace trotz der beschriebenen Revierkämpfe zuweilen ein Informationsaustausch zwischen den Geheimdiensten stattfindet, wofür es innerhalb des GRU zwischen Fancy Bear und Sandworm im Falle des Macron-Hacks 2017 Anzeichen gegeben hat (Greenberg 2019a).[110] Ferner ist untersuchungswürdig, inwieweit russische Cyberproxys womöglich auch mit HackerInnen befreundeter Geheimdienste zusammenarbeiten. Anzeichen hierfür gab es im Rahmen der Attribution der sog. ›Ghostwriter‹-Kampagne aus 2021, die die EU Russland, das US-Unternehmen Mandiant jedoch mit dem belarussischen Militär affiliierten AkteurInnen zugesprochen hat, dabei eine russische Unterstützung jedoch auch nicht kategorisch ausschloss (vgl. Roncone et al. 2021; Page 2021).

Das 2019 von Putin verabschiedete ›Sovereign Internet-Law‹ könnte dem Privatsektor zufolge zwar einerseits eine größere Kontrolle und bessere strafrechtliche Verfolgung russischer HackerInnen ermöglichen, andererseits sei jedoch bei Gruppierungen, die lediglich andere Staaten angreifen, hiervon auch weiterhin nicht auszugehen (Yakovlev 2020, S. 6–7). Dass sich russische HackerInnengruppen jedoch teilweise auch gegen nationale Behörden richten, zeigte der Leak von FSB-Überwachungswerkzeugen 2019

109 Diese Einschätzung spiegelt sich auch in der Bewertung des IISS aus 2021 wider: »*Russia's cyber strategy is dictated by its confrontation with the West, in which it sees cyber operations as an essential component of a wider information war. Its cyber governance is centralised, hierarchical and under the president's personal control*« (IISS 2021b).

110 Ein erklärungsbedürftiges Residuum wären zudem Cyberoperationen der verschiedenen Proxys, die eher dem Auftragsprofil einer anderen Geheimdienstbehörde und somit einem anderen Proxy entsprächen. Ein Beispiel wären die 2019 seitens Googles berichteten Kampagnen gegen »*Russian automotive-selling businesses, as well as real estate and finance firms*« (Greenberg 2019a), die aufgrund ihres domestischen Fokus eher in den Aufgabenbereich des FSB fallen müssten. Letzterer hat jedoch (wie z.B. im Falle des DNC-Hacks) sein Tätigkeitsspektrum selbst immer stärker erweitert und ist somit in das internationale ›Hoheitsgebiet‹ von SWR und GRU eingedrungen, weshalb ein ähnliches Verhalten auch auf GRU-Seite möglich erscheint.

(Bradbury 2019), der künftig noch schneller unterbunden werden könnte.[111] Gleiches gilt für Ransomwareoperationen, die aus russischer Sicht zu großen internationalen Widerstand hervorrufen oder ein strategisches Verhandlungsmittel darstellen können.

5.6 Demokratisches Fallbeispiel I: USA

»The attribution is a step towards holding them accountable, but it's not the last step. Addressing cybersecurity threats also requires governments and businesses to cooperate to mitigate cyber risk and to increase the cost to hackers by defending America. The U.S. will lead this effort.«
Tom Bossert, Homeland Security Advisor unter Donald Trump zur WannaCry-Attribution, zitiert in U.S. Mission Korea (2017).

Die USA stellen für die Analyse demokratischer Attributionspraktiken und die Rolle privater IT-Unternehmen eine Art ›Best Case‹ dar. Kein anderes Land ist so stark von Cyberoperationen jedweder Art betroffen wie die USA. Deren technologische Vormachtstellung, ihr hoher Grad an Digitalisierung und Vernetzung, gleichzeitig jedoch auch ihr nach wie vor defizitäres Schutzniveau zahlreicher Industriesektoren machen sie zu einem attraktiven Ziel für HackerInnen. Für die Analyse der konzeptualisierten defensiven Cyberproxy-Nutzung werden jedoch auch die Offensivkapazitäten und Handlungen der US-Administrationen von 2000 an relevant sein. Zuvor gilt es jedoch, das Attributionsverhalten unterschiedlicher US-AkteurInnen auf Grundlage des HD-CY.CON zu analysieren und im Anschluss mögliche Defensivproxys aufseiten der USA näher zu beleuchten. Die dem privaten IT-Sektor des Landes beigemessene Bedeutung bringt das obere Zitat im Zuge der WannaCry-Attribution 2017 zum Ausdruck.

5.6.1 US-Cyberattributionen: Wer macht was?

Für die USA als demokratische Fallstudie sind in erster Linie die 217 im Datensatz enthaltenen Fälle relevant, in denen (u.a.) amerikanische IT-Unternehmen zumindest eine der beiden Attributionskategorien (Initiator-Category und Initiator-Country) attribuiert haben. Darüber hinaus werden für den Vergleich technischer und politischer Attributionspraktiken der USA davon diejenigen Cyberoperationen untersucht, in denen

111 Gegen diese These spricht, dass es einen ähnlichen Leak von FSB-Daten seitens der gleichen HacktivistInnengruppierung (›Digital Revolution‹) zumindest auch noch im Jahr 2020 gegeben hat (Soschnikow 2020).

US-Ziele unter den Opfern waren und gleichzeitig (u.a.) politische AkteurInnen der USA attribuiert haben.

Diese beiden Fallgruppen werden nun entsprechend der unter 4.5 gelisteten Leitfragen genauer analysiert. Im Gegensatz zu den autokratischen Fallstudien werden AV I und AV II im Falle der Demokratien gemeinsam behandelt, da eine ähnlich strikte Trennung der Analyse hier nicht sachdienlich ist.

Zunächst wird untersucht, in wie vielen Fällen US-IT-Unternehmen einen Vorfall öffentlich machten. Die Kategorie der ›Source-Incident-Detection/Disclosure‹ dient als erster Indikator für die Proxy-Funktion der Stärkung technischer und soziopolitischer Resilienz. In 170 Fällen berichtete erstmals eine IT-Firma aus den USA über einen Cybervorfall.[112] Damit rangieren IT-Unternehmen aus den USA im Gesamtvergleich in dieser Kategorie zwar weit hinter den von den AngreiferInnen selbst veröffentlichten Vorfällen (579), aufgrund der großen Häufigkeit von DDoS-Operationen nichtstaatlicher AkteurInnen ist dies jedoch kein überraschender Befund. Im Vergleich zu weiteren Quellen, z.B. MedienvertreterInnen (87)[113] oder Drittparteien (82), liegen US-IT-Unternehmen jedoch deutlich vorne.

Bei der Betrachtung der Kodierungen amerikanischer US-Unternehmen in Richtung staatlicher AkteurInnen (Proxys und allgemein/direktstaatlich) nach Attributionsjahr wird deutlich, dass deren Anzahl über die Zeit fast exponentiell angestiegen ist und 2018 mit 42 erfassten Attributionen ihren vorläufigen Höhepunkt erreicht hat (Abbildung 32).

Abbildung 33 differenziert zwischen den beiden AngreiferInnen-Kategorien. Die im HD-CY.CON erfassten Attributionen von US-IT-Unternehmen in Richtung staatlich gesponserter AkteurInnen (Proxys) überwogen im Vergleich zu allgemein/direktstaatlich attribuierten AngreiferInnen deutlich und stiegen bis 2018 signifikant an. Zumindest der Abfall zu den Jahren 2020 und 2021 könnte dadurch erklärt werden, dass der HD-CY.CON die Angriffsjahre bis 2019 erfasst, weshalb bei einer Erweiterung um diese Jahre auch die darin getätigten Attributionen von IT-Unternehmen (in beiden Kategorien) steigen dürften.

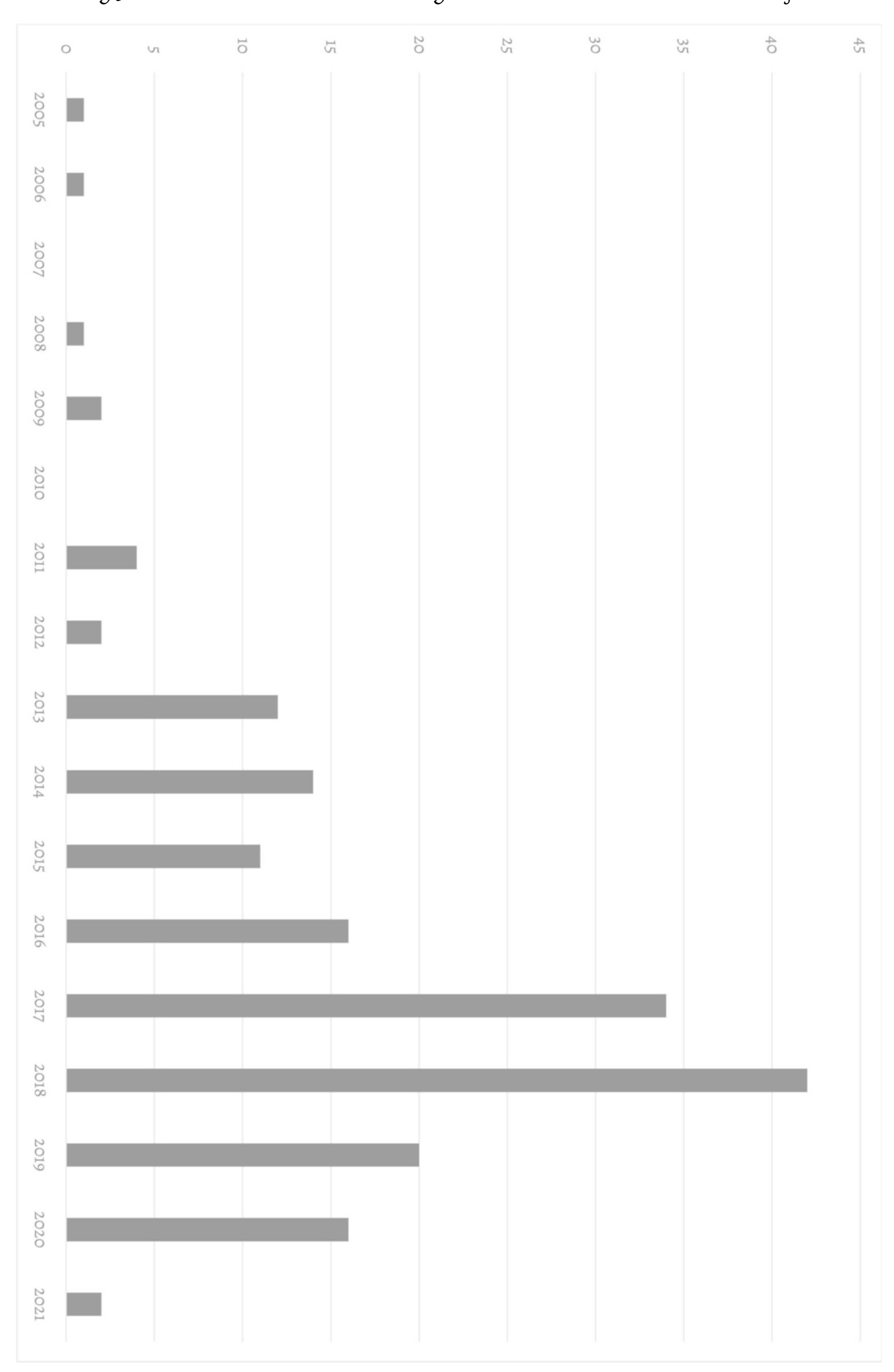
In 176 der 217 US-IT-Attributionen mit mindestens einer positiven Kodierung wurden sowohl die Initiator-Category als auch das Land des Angreifers attribuiert. ›Blurred Attributions‹ machen somit nur ca. 18,9 Prozent der US-IT-Attributionen aus.

Für die Kategorie der allgemeinen/direktstaatlichen Attributionen (20) sticht das Jahr 2016 heraus, in dem im Vergleich deutlich häufiger eine solche Zuweisung durch US-IT-Unternehmen vorgenommen wurde (7).

112 Insgesamt machten IT-Unternehmen 305 Fälle des HD-CY.CON überhaupt erst öffentlich.

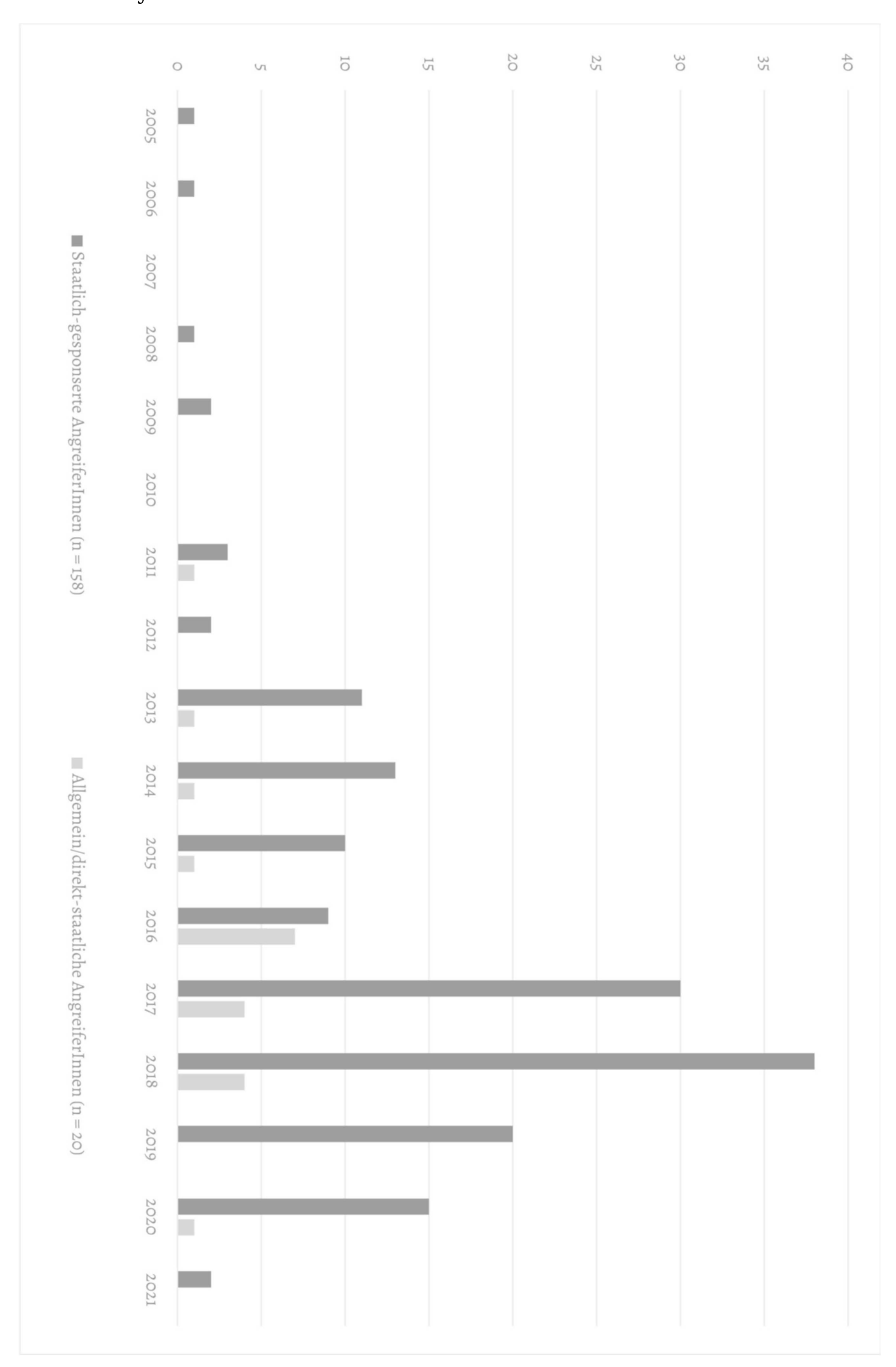
113 Diese Zahl bezieht sich auf solche Fälle, in denen MedienvertreterInnen in ihren Berichten keine weiteren Quellen bezüglich der Detektion der Operationen angaben.

Abbildung 32: US-IT-Attributionen in Richtung staatlicher AkteurInnen im Zeitverlauf



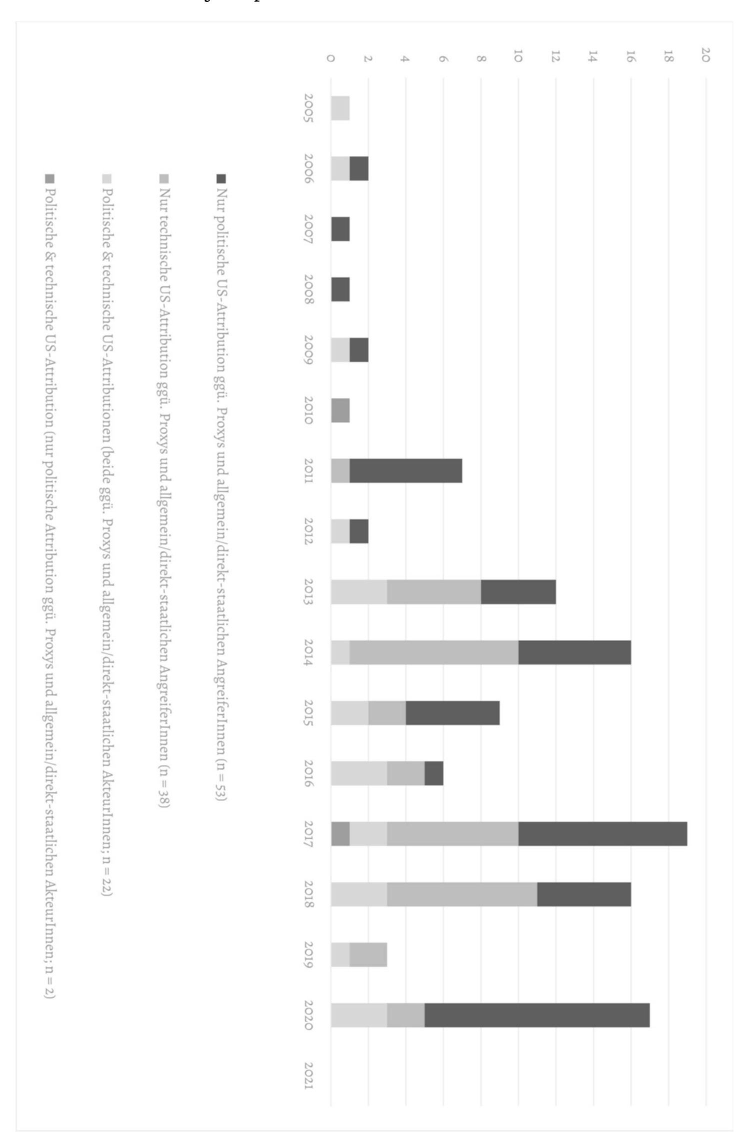
(Eigene Darstellung auf Basis des HD-CY.CON)

Abbildung 33: Staatlich affiliierte Initiator-Kategorien der US-IT-Attributionen im Zeitverlauf



(Eigene Darstellung auf Basis des HD-CY.CON)

Abbildung 34: Fälle mit sowohl politischen als auch technischen Attributionen von US-AkteurInnen für Operationen mit US-Zielen



(Eigene Darstellung auf Basis des HD-CY.CON)
Erklärung: In 53 Fällen mit US-Zielen, in denen aufseiten der USA ausschließlich politische/staatliche AkteurInnen eine Attribution vornahmen, richtete sich deren Verantwortungszuweisung gegen Proxys oder allgemeine/direktstaatliche AngreiferInnen.
In 22 Fällen mit US-Zielen, in denen aufseiten der USA sowohl politische/staatliche als auch technische AkteurInnen eine Attribution vornahmen, richteten sich deren jeweilige Verantwortungszuweisungen gegen Proxys oder allgemeine/direktstaatliche AngreiferInnen.

Dass die amerikanischen IT-Unternehmen im HD-CY.CON bislang besonders häufig staatlich gesponserte oder affiliierte Attributionen vornahmen, kann zum einen auf die prävalente Nutzung von Cyberproxys durch Autokratien hindeuten, andererseits jedoch auch auf eine mögliche Zurückhaltung der IT-Unternehmen, noch häufiger Staaten und deren Geheimdienstbehörden oder militärische Einheiten direkt verantwortlich zu machen.

Diese ersten Befunde weisen bereits auf das Vorliegen der defensiven Proxy-Funktion der Resilienzsteigerung auf soziopolitischer sowie technischer Ebene hin. Die US-IT-Unternehmen intensivierten über die Jahre ihre Threat-Research-Reports sowie ihre Verantwortungszuweisungen gegenüber staatlichen AkteurInnen zahlenmäßig erheblich. Dass es ihnen dabei jedoch nicht nur auf ›True Attribution‹ ankam, indizieren die 29 Vorfälle, in denen weder die Akteurschaft noch das Herkunftsland der AngreiferInnen attribuiert wurde und der Fokus somit auf der Detektion und Veröffentlichung technischer Details der Angriffsstrukturen lag.

In 73 der 217 Vorfälle waren US-Ziele unter den Betroffenen, somit in ca. einem Drittel der Fälle. Neben dem Fokus der US-IT-Industrie auf besonders von Cyberoperationen betroffenen einheimischen AkteurInnen und Institutionen wurde somit auch in großer Zahl für Fälle ohne US-Betroffenheit eine Verantwortungszuweisung getätigt. Auch dieser Befund stärkt die Erklärungskraft der defensiven Cyberproxy-Funktion der technischen und soziopolitischen Resilienz, auch für Ziele außerhalb der USA. Gleichwohl lässt sich dies durch den weltweiten Marktzugang führender US-IT-Unternehmen erklären, deren Aktivitäten und somit auch Threat-Research-Bemühungen nicht nur auf die nationale Ebene beschränkt sind.

Abbildung 34 zeigt alle Fälle mit US-Zielen auf, in denen entweder politische oder technische US-AkteurInnen Attributionen in Richtung staatlicher AkteurInnen vorgenommen haben, sowie Fälle, in denen beide Seiten eine solche Verantwortungszuweisung äußerten.

Die Anzahl an Vorfällen mit US-Zielen, in denen ausschließlich politische US-Attributionen in Richtung staatlicher Proxys oder direktstaatlicher AngreiferInnen verzeichnet wurde, übersteigt mit 53 den der umgekehrt ausschließlich technischen Attributionen dieser Art (38).

In Kombination traten technische und politische Attributionen gegen staatlich affiliierte AngreiferInnen in 22 Fällen mit US-Zielen auf.

Von den 53 Fällen mit ausschließlich politischer Verantwortungszuweisung lassen sich 49 in die Kategorie der ›True Attribution‹ einsortieren, nur in vier Fällen wurde das Ursprungsland der Operation nicht genauer benannt. Dies weist darauf hin, dass, wenn politische AkteurInnen in Demokratien ihre ansonsten im Vergleich zu IT-Unternehmen eher bestehende Attributionszurückhaltung aufgeben (siehe Kapitel 5.2.3, Abbildung 24), sie die Verantwortlichen überwiegend auch konkret benennen. Gleichzeitig könnte diese Beobachtung als Hinweis darauf gewertet werden, dass Demokratien wie die USA eben nicht nur dann attribuieren, wenn zuvor bereits eine ähnliche Verantwortungszuweisung seitens des eigenen IT-Sektors erfolgte. Somit schränkt dies die Erklärungskraft der Proxy-Funktion ›Schaffung von Legitimation politischer Attributionen‹ für die USA ein. Andererseits dienen für die zumindest zeitweilige Wirkung der kon-

zeptualisierten Cyberproxy-Funktion der ›Reduzierung politischen Handlungsdrucks‹ die 38 Fälle rein technischer US-Attributionen als Indikator.

Dass in lediglich zwei Fällen US-IT-Unternehmen den Verantwortungszuweisungen politischer/staatlicher US-AkteurInnen nicht folgten, deutet eine signifikante Kohärenz der US-Attributionen an. Unter den Fällen mit signifikant unterschiedlicher Attribution der Initiator-Category sticht besonders der Sony-Hack aus 2014 heraus: Hier wurde als zusätzliche Attribution-Basis ›Contested Attribution‹ kodiert, da US-IT-Experten wie Bruce Schneier und Jeffrey Carr die bereits am 19. Dezember durch das FBI erfolgte Verantwortungszuweisung in Richtung Pjöngjang kritisch bewerteten (Schneier 2014; Collier 2018). Andere, auch heute noch wirtschaftlich erfolgreiche US-IT-Unternehmen wie FireEye und CrowdStrike bestätigten jedoch die politische Attribution. Dass öffentlich gemachte Attributionen und speziell die des Sony-Hacks von US-Behörden in der Folge nicht mehr entsprechend kontestiert wurden, liegt laut diesen Unternehmen an der Weiterentwicklung der Branche, da sich mittlerweile weitgehend »*die Spreu vom Weizen getrennt*« habe (Collier 2018). Besonders der Vorwurf, Attribution im Cyberspace und somit ein Teil des Geschäftsmodells von Unternehmen wie FireEye & Co. seien kaum möglich, wurde von Letzteren wenig überraschend entschieden zurückgewiesen.

Die Ausführungen des Sony-Hacks deuten darauf hin, dass in vereinzelten, für die USA jedoch seltenen Fällen die IT-Community der Attribution ihrer Regierung auch aktiv widersprechen kann. Dabei handelte es sich jedoch eher um Einzelakteure, deren Geschäftsbeziehungen zur US-Regierung nicht mit denen der größeren IT-Unternehmen vergleichbar gewesen wären. Letztere setzten sich in der Branche der technischen Attribution eindeutig durch, was auch durch ihre hohe Resonanz in journalistischen Berichten zum Ausdruck kommt. Dass sich deren Verantwortungszuweisungen stets mit denen politischer Akteure, vor allem im Rahmen von Anklageerhebungen, deckten, kann für deren Wahrheitsgehalt und Plausibilität, in Teilen jedoch auch für übereinstimmende Interessen sprechen.

In den 22 Fällen gemeinsamer US-Attributionen in Richtung staatlicher AngreiferInnen mit US-Zielen erfolgte elfmal die politische Verantwortungszuweisung vor der technischen, die umgekehrte Reihenfolge wurde achtmal verzeichnet, in den übrigen drei Fällen war die zeitliche Abfolge unklar. Aufseiten der IT-Unternehmen dominierten Threat-Research-Berichte mit technischen Details das Bild der verzeichneten Attribution-Types. Die politischen US-Attributionen waren dagegen durch Anklagen sowie Verantwortungszuweisungen in Form von Medienzitaten geprägt.

Ein Abgleich der zeitlichen Abfolge der Attributionen in Relation zu diesen verschiedenen Attributionstypen ergab keine auffälligen Muster. Anders sieht es jedoch für die Kategorie der Anklageerhebungen alleine betrachtet aus: Während nach der ersten Anklageerhebung 2014 unter Barack Obama lediglich vier weitere Anklagen gegen ausländische Hacker erhoben wurden, deren Operationen für den HD-CY.CON relevant sind, stieg diese Zahl unter Trump auf 23 an.[114] In keinem der Fälle mit US-Anklage wurde ein gewaltsamer HIIK-Konflikt zwischen den USA und dem attribuierten Initiator-Country

114 Im Datensatz bezogen sich in manchen Fällen mehrere Cyberoperationen auf dieselbe Anklage, wenn in diesen mehrere Operationen zur Anklage gebracht wurden.

verzeichnet. Die USA erhoben lediglich 2020 Anklage gegen den GRU (Sandworm) aufgrund der Sabotageakte gegen die ukrainischen Stromversorger 2015/2016, ukrainische Finanzinstitutionen 2016 sowie NotPetya 2017, wobei für die Dyade Ukraine-Russland ein gewaltsamer HIIK-Konflikt verzeichnet wurde.

Auf Basis dieser Befunde kann die Cyberproxy-Funktion der ›Schaffung von Legitimation politischer Attributionen‹ für die USA nicht hinreichend bekräftigt werden, zumindest nicht im Sinne der in Kapitel 3.2.2 vorgelegten, auf der zeitlichen Abfolge basierenden Argumentationsweise, dass vor allem vorab erfolgte technische Attributionen nachgelagerten politischen Attributionen zu mehr Glaubwürdigkeit verhelfen könnten.

Tabelle 18 listet die zehn am häufigsten im Datensatz attribuierenden US-IT-Unternehmen auf, bezogen auf alle Fälle und somit nicht nur Operationen gegen US-Ziele.

Unter den zahlreichen im Datensatz verzeichneten US-Unternehmen sticht FireEye deutlich mit 74 Fällen heraus, in denen eine Attribution des Unternehmens verzeichnet wurde, gefolgt von Symantec und Palo Alto. FireEye, Recorded Future sowie CrowdStrike attribuierten im Gegensatz zu Symantec und Palo Alto deutlich häufiger konkrete AkteurInnen, während die beiden letztgenannten Unternehmen bislang zumeist nur ›Blurred Attributions‹ vornahmen. Gleiches gilt auch für die übrigen US-Unternehmen der Rangliste im Vergleich zu Symantec und Palo Alto.

Tabelle 18: Die am häufigsten als Attributionsquelle verzeichneten US-IT-Unternehmen

Rang	Unternehmen	Vorkommen im HD-CY.CON
1	FireEye	69 (Threat-Reports); 5 (Medienzitate)
2	Symantec	39 (Threat-Reports)
3	Palo Alto	22 (Threat-Reports); 1 (Medienzitate)
4	Recorded Future	15 (Threat-Reports); 2 (Medienzitate)
5	CrowdStrike	10 (Threat-Reports); 6 (Medienzitate)
6	McAfee	10 (Threat-Reports)
7	Proofpoint	9 (Threat-Reports)
8	Secureworks	7 (Threat-Reports)
9	Dragos	5 (Threat-Reports); 2 (Medienzitat)
10	Threatconnect	5 (Threat-Reports); 1 (Medienzitate)
11	Volexity	5 (Threat-Reports)

(Eigene Darstellung auf Basis des HD-CY.CON)

Auch im Hinblick auf Vorfälle, in denen sowohl die AngreiferInnenkategorie als auch das Herkunftsland attribuiert wurde (›True Attribution‹), rangiert FireEye deutlich vor

Zur Ermittlung der hier genannten Zahlen wurde folgende Liste auf Relevanz für den HD-CY.CON überprüft und die Anklagen aus 2020 mittels eigener Recherche hinzufügt: https://docs.google.com/document/d/1sipdsjWkDlT9xmbbQQ3wKfanmETS-N_4VD60H2ssfgQ/edit.

Symantec auf dem ersten Platz. Dieser augenscheinliche Widerspruch zur zuvor getätigten Aussage erklärt sich dadurch, dass die Symantec-Attributionen oftmals nur in Kombination mit weiteren Quellen, z.B. in Medienberichten zitierten ExpertInnen, als konkrete Verantwortungszuweisungen gewertet werden konnten, dann aber in vielen Fällen.

Nachfolgend werden zwei Cyberoperationen herausgegriffen, in denen sich Hinweise auf eine Kooperation zwischen dem US-IT-Sektor und US-Behörden finden lassen bzw. sich die Attributionen inhaltlich aufeinander bezogen haben. Hierdurch sollen gleichzeitig zwei der am häufigsten im Datensatz erfassten US-Unternehmen und somit potenzielle Cyberproxys der USA genauer vorgestellt werden: FireEye und CrowdStrike.

1. Attributionsfall: APT1-Bericht aus 2014 (Mandiant und FireEye)

Der für die private Cyberattributionsbranche bedeutende Bericht der US-IT-Firma Mandiant (heute zu FireEye gehörend) mit dem Titel »*APT1: Exposing One of China's Cyber Espionage Units*«, der im Februar 2013 veröffentlicht wurde, legte den Grundstein für alle weiteren technischen Attributionsberichte. Im Bericht wurde nicht nur eine spezifische PLA-Einheit als konventionelles Pendant der Hackergruppe bezeichnet, sondern einzelne Mitglieder wie Wang Dong (aka ›Ugly Gorilla‹) wurden auch als Angehörige der APT identifiziert. Unterstützt wurden diese Zusammenhänge durch IT-forensische Evidenzen, die Mandiant in zuvor noch nicht dagewesener Weise zusammengetragen und veröffentlicht hatte. So wurden der ›Attack-Lifecycle‹, die Angriffsinfrastruktur sowie die verwendete Malware im Detail beschrieben.

Der Bericht fand auch in der US-Politik großen Widerhall: Noch am Tag der Veröffentlichung bestätigte der damalige Vorsitzende des ›United States House Permanent Select Committee on Intelligence‹, Mike Rogers, dass die Erkenntnisse des Berichtes mit denen des Geheimdienstkomitees übereinstimmten (FireEye 2016, S. 7). Zudem beschuldigte im Mai 2013 auch das Pentagon in einem durchgesickerten Bericht chinesische Militärhacker umfangreicher Cyberspionage gegen US-Waffensysteme mit erheblichen sicherheitspolitischen Implikationen (Nakashima 2013b).

Das Momentum schien im Vorfeld eines bevorstehenden Gipfels zwischen Obama und Xi im Juni 2013 somit aufseiten der USA zu sein. Im Mai enthüllte Edward Snowden jedoch seine internen NSA-Unterlagen und verschlechterte damit die US-Verhandlungsposition im Feld der Cyberspionage erheblich, auch wenn es sich dabei nicht um die im Fokus stehende ökonomisch motivierte Spionage handelte.

Als am 19. Mai 2014 schließlich das US-Justizministerium nachzog und das erste Mal in Form einer Anklage ausländische Hacker als Militärangehörige eines anderen Staates identifizierte, bahnte sich eine Intensivierung des politischen Drucks der USA an. Dabei lagen die Parallelen zwischen den Erkenntnissen des Mandiant-Berichtes sowie den in der Anklageschrift aufgelisteten Attributionsevidenzen auf der Hand. Das Ministerium benannte dieselbe PLA-Einheit sowie in Teilen auch dieselben Akteure (z.B. Wang Dong) als verantwortlich für jahrelange Cyberspionageoperationen gegen US-Unternehmen (DoJ 2014a). Zwar wurde in der Anklageschrift der Mandiant-Bericht nicht erwähnt, jedoch bezieht sich ein Gesetzesentwurf vom 14. Juli 2014, der dem US-Kongress vorge-

legt wurde, auf die Attributionserkenntnisse der Unternehmen Mandiant und CrowdStrike. Letzteres hatte zuvor eine weitere PLA-Einheit (61486) als die APT »*Putter Panda*« identifiziert (US Government 2014). Es kann daher von einem Informationsaustausch zwischen Mandiant und den US-Behörden im Vorfeld der Anklageerhebung ausgegangen werden, wenn auch ein Blogpost von FireEye nahelegt, dass auch das Unternehmen vor der Veröffentlichung nicht über sämtliche Punkte Bescheid wusste (Bejtlich 2014).

Dennoch bleibt festzuhalten, dass der Mandiant-Bericht der anschließenden Anklage gewissermaßen den Weg ebnete und zu noch größerer Glaubwürdigkeit verhalf, gerade in Folge der dazwischen liegenden Snowden-Enthüllungen. Zudem erweiterte der Bericht den politischen Handlungsspielraum der Obama-Administration, da hierdurch erstmals umfangreiche technische Beweise die chinesische Wirtschaftsspionage belegten. Hierdurch verhalf die zuerst getätigte Attribution der IT-Community entgegen den zahlenmäßigen Trends des HD-CY.CON der nachgelagerten politischen Attribution zudem zu größerer Legitimation. Ferner ist von einer im Vorfeld stattgefundenen Kooperation zwischen den staatlichen Behörden und dem Privatsektor auszugehen. Inwiefern Erstere bereits vor der Veröffentlichung des Mandiant-Berichtes hierüber Bescheid wussten oder dessen Erstellung und Veröffentlichung sogar unterstützten, kann an dieser Stelle jedoch nicht beurteilt werden.

Jedenfalls haben sowohl der potenzielle staatliche Auftraggeber/Sponsor als auch der Proxy in diesem Beispiel einen beidseitigen Vorteil aus ihren jeweiligen Attributionsbemühungen gezogen. FireEye verschaffte sich einen immensen Startvorteil im Feld der öffentlich-technischen Attribution gegenüber den Mitbewerbern und erhöhte dadurch die eigene Reputation. Das US-Justizministerium schickte durch die erstmalige Anklageerhebung ein deutliches Signal in Richtung Peking, dass nicht nur private IT-Unternehmen chinesische Cyberoperationen verstärkt in den Fokus ihrer Analysen nahmen, sondern auch der amerikanische Staat von nun an proaktiver gegen diese vorgehen würde. Wird das 2015 geschlossene Obama-Xi-Abkommen als Resultat dieser Prozesse betrachtet, kann diese ›Naming-and-Shaming‹-Strategie in diesem Falle als erfolgreich bewertet werden.

Das Unternehmen FireEye wurde 2004 in Kalifornien gegründet. Ab 2009 wurde es u.a. auch durch In-Q-Tel gesponsert, ein offizielles Non-Profit-Unternehmen, das jedoch aus dem Haushalt der CIA finanziert wird. In-Q-Tel investiert in für die staatliche Geheimdienstarbeit relevante Technologien und sichert diesen somit gewissermaßen ein Prärogativrecht hierauf (O'Hara 2005). Auf der FireEye-Website wurde ein Partner von In-Q-Tel bezüglich des Investments folgendermaßen zitiert:

> »FireEye is a critical addition to our strategic investment portfolio for security technologies […] FireEye offers a valuable combination of next-generation malware protection, and its approach to detecting and defeating malware is unique and potenzially game changing.« (zitiert in: FireEye 2009)

Laut FireEye-Gründer Ashar Aziz versprach die Zusammenarbeit mit In-Q-Tel die Möglichkeit, »to provide the U.S. Intelligence-Community with a technology solution to help defeat cyber threats, and to directly address critical national security needs« (zitiert in: FireEye 2009). Dieses frühe Ausmaß an geheimdienstlicher Involvierung in die Tätigkeiten FireEyes legt zumindest nahe, dass die Veröffentlichung des Mandiant-Reportes

bereits im Rahmen dieser Kooperation gemeinsam orchestriert, zumindest aber abgestimmt wurde. FireEye und Mandiant hatten 2012 eine ›strategische Allianz‹ beschlossen, auch wenn die Übernahme erst zum 30. Dezember 2013 offiziell erfolgte (Wiegand 2014). Somit kann zumindest für diesen Fall die angestrebte Cyberproxy-Funktion der ›Schaffung von Legitimation‹ der nachgelagerten politischen Attribution als erklärungskräftig angesehen werden.

Die eigene Marktstellung im Bereich der Threat-Intelligence baute FireEye 2016 durch die Übernahme des IT-Unternehmens iSight Partners weiter aus. Dieses hatte 2014 durch seine Berichte über iranische Cyberoperationen (›Operation Newscaster‹; Nakashima 2014) sowie die russische Hackergruppierung Sandworm auf sich aufmerksam gemacht (Zetter 2014). Weitere Belege für eine zumindest zeitweilige Zusammenarbeit zwischen FireEye bzw. dem übernommenen Unternehmen Mandiant und staatlichen Behörden, finden sich im Falle des Spionagevorfalls gegen den US-Gesundheitsdienstleister Premera Blue Cross aus dem Jahr 2014. Hier arbeitete das FBI mit Mandiant zusammen, das sich »*specializes in tracking and blocking attacks from state-sponsored hacking groups, particularly those based in China*« (Krebs 2015). Die jeweilige Kooperation scheint somit gezielt mit Unternehmen eingegangen zu werden, deren spezifisches Forschungsprofil zu den vermuteten AngreiferInnen passt.

Mit 74 verzeichneten Fällen, in denen Attributionsevidenzen von FireEye im HD-CY.CON erfasst wurden, rangiert das Unternehmen an der Spitze (s. Tabelle 18), auch wenn der Datensatz keine Vollständigkeit beansprucht. Dass in der großen Mehrzahl der Fälle AkteurInnen aus konkreten Ländern attribuiert wurden, unterstreicht die vermutete Proxy-Funktion des Signalings bzw. der Reduzierung des politischen Handlungsdrucks, da in den Berichten eben nicht nur technische Details zu den verwendeten ›Indicators of Compromise‹ (IOCs) veröffentlicht wurden. Bemerkenswert ist jedoch, dass zahlreiche Attributionsberichte auch Fälle ohne US-Ziele betrafen. Dies spricht entweder für eine eingeschränkte Proxy-Rollenübernahme durch FireEye im Sinne der hier vorgestellten Logik oder könnte bedeuten, dass sich diese Attributionen nicht nur auf US-Ziele beschränken müssen, sondern im Sinne des ›Naming-and-Shamings‹ sowie der Steigerung der technischen Resilienz der Adressaten auch Operationen außerhalb der USA inkludieren. Dass die Mehrzahl der Vorfälle mit China, Russland, Iran und Nordkorea in Richtung der sog. ›Big Four‹ der autokratischen Cyberoffensive attribuiert wurden (McNamara 2021), spricht eher für die zweite These, da deren Attribution für die zwei genannten Proxy-Funktionen zielunabhängig erfolgen kann.

2. Attributionsfall: DNC-Hack/Leak

Als zweite Einzelfallstudie wird der DNC-Hack/Leak im Rahmen der russischen US-Wahlbeeinflussung 2016 vorgestellt und die Rolle des Unternehmens CrowdStrike beleuchtet.[115]

115 Auch wenn im weiteren Verlauf der Ereignisse besonders die US-IT-Unternehmen SecureWorks und ThreatConnect ebenfalls wichtige Attributionsevidenzen veröffentlichten, spielte CrowdStrike doch die zentrale Rolle in der Detektion, Bekämpfung und Attribution von Fancy Bear.

Nachdem das FBI in den vorangegangenen Jahren bereits versucht hatte, die Hackergruppierung Cozy Bear aus den Netzwerken des Weißen Hauses und des State Departments zu entfernen,[116] wurde ein Agent der Behörde im September 2015 auf deren Kompromittierung eines DNC-Netzwerkes aufmerksam (Lipton et al. 2016). Dessen mehrfache Warnungen blieben jedoch aufgrund einer nicht weitergeleiteten Nachricht weitgehend unbeachtet. Am 19. März 2016 erhielt zudem der damalige Kampagnenmanager Clintons, John Podesta, eine als Google-Sicherheitswarnung getarnte Phishing-Mail. Infolge eines angeblichen Tippfehlers des von Podesta bezüglich der Vertrauenswürdigkeit der Mail befragten IT-Mitarbeiters aktivierte er den Link und ermöglichte den Hackern Zugang zu seinem Account (Lipton et al. 2016). Im späten April 2016 wurde die IT-Abteilung des DNC schließlich doch noch misstrauisch und beauftragte einerseits die Sicherheitsfirma CrowdStrike mit der Untersuchung und Bereinigung der eigenen Netzwerke und bestätigte andererseits gegenüber dem FBI dessen Ursprungsverdacht. CrowdStrike installierte daraufhin eine spezielle Monitoring-Software, die die Analyse der verdächtigen Hacker-Aktivitäten erlaubte (Strauss 2016)

Auf dieser Grundlage gab die Firma am 15. Juni schließlich bekannt, dass sowohl Cozy als auch Fancy Bear zeitweilig in den DNC-Netzwerken aktiv gewesen seien. Während die FSB-Gruppierung Cozy Bear dies jedoch wie erwähnt bereits seit 2015 und bis zum Zeitpunkt der Entdeckung durch die Nutzung eingebauter Windows-Tools weitgehend unauffällig tat, drang die GRU-Gruppe Fancy Bear erst im März 2016 für wenige Wochen ebenfalls in die Netzwerke ein (Lipton et al. 2016). Im ersten Fall handelte es sich um eine breitere und unspezifische Spear-Phishing-Kampagne, die zudem *»a long list of American government agencies, Washington nonprofits and government contractors«* anvisierte (Lipton et al. 2016). Dies entspricht der Cozy Bear zugesprochenen Vorgehensweise sowie allgemeinen russischen Interessenlagen.

Als schließlich am 10. Juni in einer konzertierten Aktion CrowdStrike sämtliche DNC-Rechner von der kompromittierten Software säuberte, war der eigentliche DNC-Hack beendet, nicht jedoch die mit ihm verbundene russische Einflussnahme. Danach entwickelte sich der ursprüngliche ›DNC-Hack‹ zum erst richtig öffentlichkeitswirksamen ›DNC/Hillary-Leak‹. Nachdem das DNC beschloss, an die Öffentlichkeit zu gehen, daraufhin die Washington Post am 14. Juni das erste Mal öffentlich den DNC-Hack mit den beiden russischen Hackergruppierungen in Verbindung brachte (Nakashima 2016) und CrowdStrike einen detaillierten Bericht über den Vorfall veröffentlichte (Alperovitch 2016), behauptete ein Blogger namens ›Guccifer 2.0‹, CrowdStrike würde sich irren und er selbst sei der Verantwortliche. Amerikanische IT-Sicherheitsexperten zweifelten früh an der Authentizität dieses angeblichen Einzeltäters. Stattdessen bewerteten sie es als ein versuchtes Ablenkungsmanöver des russischen Geheimdienstsektors (Groll 2016).

Insgesamt wurden den durch Wikileaks im Juli veröffentlichten E-Mails des DNC die größte Brisanz und Öffentlichkeitswirksamkeit zugesprochen, die Seite DCLeaks erhielt erst hierdurch größere Aufmerksamkeit. Auch wenn Guccifer 2.0 und DCLeaks angaben, entweder rumänischer Herkunft oder gar patriotische amerikanische Hacker zu sein, wurden diese Behauptungen durch eingehende Analysen von ThreatConnect früh

116 Wie später bekannt wurde, hatte zuvor bereits der niederländische Geheimdienst das FBI hierauf hingewiesen, wie auch beim DNC-Hack (Segal 2018).

in Zweifel gezogen und auf Grundlage IT-forensischer Indikatoren Verbindungen beider Akteure zu Fancy Bear hergestellt (Threat Connect Research Team 2016).

Im weiteren Verlauf setzten die USA mit Robert Mueller einen Sonderermittler ein, der bei der russischen Beeinflussung auch die Rolle der Trump-Administration von 2017 bis 2019 aufarbeitete. Dessen Ermittlungen führten im Februar 2018 schließlich zu einer ersten Anklageerhebung gegen 13 russische Personen und drei Firmen, darunter etwa der mutmaßliche Leiter der Internet Research Agency (IRA) in St. Petersburg, Jewgeni Prigoschin. Den Angeklagten wurden unterschiedliche Beteiligungen an der russischen Wahlbeeinflussung 2016 angelastet, z.B. Identitätsdiebstahl von US-BürgerInnen, um in deren Namen polarisierende Nachrichten auf Social-Media-Plattformen zu veröffentlichen, aber auch Kontakte zum damaligen Wahlkampfteam von Donald Trump (Apuzzo und LaFraniere 2018). Die für diese Arbeit noch interessantere Anklageerhebung erfolgte jedoch im Juli 2018: Darin klagten die USA 12 russische GRU-Agenten an, die für die Hack-and-Leak-Operation gegen das DNC sowie das DCCC verantwortlich gewesen sein sollen. In der Anklageschrift wird CrowdStrike als »*Company 1*« bezeichnet und dessen Rolle bei der Entdeckung, Abwehr und Aufarbeitung der Operation in der Folge umfassend beschrieben (DoJ 2018b). Gleiches gilt für die sog. ›Mueller-Reports‹ des Sonderermittlers, der als Abschluss seiner Tätigkeit alle Ergebnisse zusammenfasste (Mueller 2019b; Mueller 2019a).

Zur politisch-rechtlichen Aufarbeitung der Wahlbeeinflussung zogen die ErmittlerInnen somit die Befunde von CrowdStrike umfassend heran, vermutlich auch, um den Berichten/Anklagen eine gewisse Neutralität zu verleihen. Somit kann für den DNC-Hack die zumindest intendierte Proxy-Funktion der ›Schaffung von Legitimation politischer Attributionen‹ auf ideeller und republikanischer Ebene durch CrowdStrike gegenüber domestischen AkteurInnen als noch bedeutender eingestuft werden als im Falle der Anklageerhebung 2014 gegen APT1, bei der parteipolitische Konfliktlinien eine weitaus geringere Rolle spielten.

Interessant ist daher das am 5. Juni 2020 auf der Firmenwebseite veröffentlichte Statement von CrowdStrike zur eigenen Zusammenarbeit mit dem FBI. Darin werden die Abläufe und Ereignisse um den DNC-Hack explizit aus Sicht der Firma berichtet. Zudem werden Fragen bezüglich der eigenen Rolle in den staatlichen Ermittlungen beantwortet. Wichtig war es dem Unternehmen offensichtlich, sowohl das eigene Primäransinnen des Schutzes der KlientInnen als auch die eigene parteipolitische Neutralität hervorzuheben. Darüber hinaus wurde im Statement klargestellt, dass die Leitung von CrowdStrike keine Beziehungen in die Ukraine unterhalten würde und sich die DNC-Server nie in physischem Besitz des Unternehmens befunden hätten. Die Anmerkungen sind konkrete Entgegnungen auf die zuvor zirkulierten Behauptungen der Trump-Administration, CrowdStrike habe im Rahmen einer ukrainischen Verschwörung die Beweise gegen Russland selbst erfunden (Bajak 2019). Die Erklärung erscheint als eine Art Balance-Akt zwischen Demokraten und Republikanern als potenziellen Wahlsiegern elf Monate später: die Betonung der eigenen Parteilosigkeit als Handreichung gegenüber den Republikanern, das Zurückweisen der Verschwörungstheorien jedoch als gleichzeitige Abgrenzung von deren Behauptungen. Trump stellte CrowdStrike somit gewissermaßen als Proxy der Demokraten mit Verbindungen in die Ukraine dar, um die Glaubwürdigkeit des Unternehmens zu diskreditieren. Jedoch muss an dieser

Stelle auch konstatiert werden, dass die ganze Affäre aus Sicht des CEOs George Kurtz dem Unternehmen wohl nicht nur geschadet, sondern auch zusätzliche Publicity eingebracht hat (Schubarth 2021). Gleiches indiziert die infolge der Fancy-Bear-Attribution gestiegene Auftragslage des Unternehmens (Au-Yeung 2019).

Zuletzt kann als zumindest zeitweiliger Cyberproxy das US-Unternehmen Recorded Future diskutiert werden. 2009 gegründet, erhielt das damalige Start-up die notwendige Finanzierung von Google und In-Q-Tel (Shachtman 2010). Während zu Beginn noch dessen Foresight-Aktivitäten auf Open-Source-Basis im Fokus standen, wodurch sich auch das Interesse Googles erklären lässt, standen speziell ab 2017, dem Gründungsjahr der hausinternen Insikt Group, die technischen Attributionsberichte vermehrt im Vordergrund. Im Rahmen der Gründung der Insikt Group wurde zudem die US-Geheimdienstvergangenheit ihres Leiters, Levi Gundert, gezielt hervorgehoben (Recorded Future 2017). Wie im Kapitel zu den chinesischen Proxys aufgezeigt, attribuierte die Insikt Group insbesondere chinesische APTs und brachte sie direkt mit militärischen oder geheimdienstlichen Einheiten in Verbindung. Es kann somit auch hier zumindest eine in Teilen vorhandene Staat-Proxy-Beziehung plausibilisiert werden. Inwiefern auch der Zeitpunkt der verstärkten Attributionen durch Recorded Future dem härteren Vorgehen der Trump-Administration gegenüber China entsprechen könnte, wird Gegenstand der Analyse der UV sein.

Neben diesen exemplarischen Fallbeispielen ist zudem die Strafanzeige des FBI (Juni 2018) gegen die nordkoreanischen Hacker der Wiper-/Ransomware-Operation WannaCry aus 2017 von Interesse: Diese verweist an zahlreichen Stellen explizit auf die umfangreiche Arbeit privater IT-Unternehmen wie Mandiant, Symantec, Novetta, Kaspersky, BAE Systems und RiskSense. Dabei werden deren technische Evidenzen aufgelistet, um die Tatbestandsmerkmale und deren Erfüllen seitens der Angeklagten für den konkreten Fall zu erhärten. Es wird den Erkenntnissen der IT-Community offensichtlich eine hohe Glaubwürdigkeit zugesprochen bzw. davon ausgegangen, dass deren Inklusion die Legitimität der Strafanzeige selbst steigern wird. WannaCry ist daher ein Beispiel für die Proxy-Funktion der ›Schaffung von Legitimation politischer Attributionen‹, auch wenn nicht davon ausgegangen wird, dass besagte IT-Unternehmen zu ihren Untersuchungen erst durch US-Behörden aufgefordert oder ermutigt werden mussten. Die Erwähnung der Unternehmen in staatlichen Anklageschriften oder Strafanzeigen dürfte deren Reputation und Ansehen eher noch steigern, was somit den notwendigen gegenseitigen Nutzen dieses Beziehungsarrangements zwischen Staat und Privatakteur unterstreicht. Gleichzeitig wird die während der Trump-Präsidentschaft forcierte ›Attribution-by-Indictment‹-Strategie hinsichtlich ihres tatsächlichen Abschreckungseffektes kritisiert und argumentiert, dass der Verlust darin zumindest implizit oftmals eingestandener Attributionsfähigkeiten und Strategien der US-Behörden deren Nutzen übersteigen würde (Machtiger 2020). Die hier angeführten Nutzungsmethoden von Open-Source-Informationen wie Social-Media-Profilen der Hacker dürften zum Zeitpunkt der Anklage jedoch auch der russischen Seite bereits bekannt gewesen sein. Die gleichzeitig angeführte Kritik, dass diese Anklagen oftmals keine wirklich neuen Erkenntnisse offenlegen und sich in erster Linie auf bereits öffentliche Evidenzen des Privatsektors stützen würden, kann daher als ein direkter Widerspruch gewertet werden (s. Machtiger 2020). Grundlegend wird jedoch wohl zurecht in Frage gestellt, ob die Anklage einzelner Indi-

viduen, wie sie normalerweise eher genuinen Kriminellen vorbehalten ist, das adäquate Mittel zur Abschreckung staatlich gesponserter HackerInnen darstellen kann. Stattdessen wird die präventive bzw. defensive Zusammenarbeit des FBI und Microsofts zur Zerschlagung der Trickbot-Malware-Infrastruktur als positives Beispiel angeführt, wie auf staatlich geführte Cyberoperationen reagiert werden sollte.

Tabelle 19: Ausprägung der AV I auf Grundlage des HD-CY.CON für die USA

Starke Ausprägung	Mittlere Ausprägung
Steigerung der soziopolitischen Resilienz (Threat-Research-Berichte von US-Unternehmen hinsichtlich Social-Engineering-Taktiken sowie Hack-and-Leak-Operationen, z.B. DNC-Hack)	Schaffung von Legitimation (nachgelagerter) politischer Attribution (Bewertungsgrundlage: Qualitative Attributionsbeispiele)*
Steigerung der technischen Resilienz (Threat-Research-Berichte von US-Unternehmen im Hinblick auf adressierte US-Wirtschaftszweige, z.B. APT1-Bericht)	Reduzierung des politischen Handlungsdrucks/Signaling (dauerhaft; Fälle mit ausschließlich technischer Attribution) bzw. Erweiterung des Handlungsspielraums (z.B. APT1-Bericht vor 2014-Anklage)

(Eigene Darstellung)
*Die Bewertung der Erklärungskraft orientiert sich hier stärker an den vorgestellten Fallstudien. Entsprechend der rein quantitativen Bewertung der Attributionsreihenfolge müsste die Erklärungskraft eher als schwach eingestuft werden.

In jüngster Zeit wurde jedoch auch von gegensätzlichen Interessen zwischen US-Behörden und Unternehmen berichtet. So kann die angestrebte technische Resilienz durch Offenlegung der Angriffe und IOCs den Attributionspraktiken von Geheimdiensten zeitweilig auch entgegenwirken (Bing 2017a). Jüngstes Beispiel hierfür ist die durch Google veröffentlichte Cyberoperation eines mutmaßlichen Five-Eye-Mitgliedes zur Terrorabwehr im März 2021, die durch den technischen Bericht vermutlich nicht mehr weitergeführt werden konnte (O'Neill 2021). Die Berichterstattung zu diesem Vorgang legte nicht nur diesen vermeintlichen Interessenskonflikt zwischen Googles ›Project Zero"[117] und westlichen Geheimdiensten nahe, sondern implizierte auch innerhalb des Unternehmens Uneinigkeiten bezüglich der Abwägung der eigenen Veröffentlichungen (O'Neill 2021). Der Vorgang wurde auch deshalb als ungewöhnlich eingestuft, da besonders größere Firmen zumindest in den USA den Behörden vor einer Veröffentlichung Bescheid geben und diese zumindest hinausgezögert werden kann, wenn geheimdienstliche Operationen dies erfordern (Bing 2017a).

Auf Grundlage der qualitativ gewonnenen Erkenntnisse können für die USA prinzipiell alle konzeptualisierten Cyberproxy-Funktionen einzelne Aspekte der hier vorgestellten Attributionspraktiken erklären (Tabelle 19). Deren Prävalenz lässt sich jedoch weniger eindeutig voneinander abgrenzen als im Falle der autokratischen Cyberproxys, was

117 Das Projekt hat sich der Aufdeckung und öffentlichen Analyse von Zero-Day-Exploits verschrieben.

die weniger distinkten Trends des US-Attributionsverhaltens im HD-CY.CON verdeutlichen.

5.6.2 Die Cyberakteursumwelt der USA

Die USA waren schon immer die technologisch führende Nation im Cyberspace. Das heutige Internet entstand als Nachfolger des ›Advanced Research Projects Agency Network‹ (ARPANET), einem Computer-Netzwerk, das Ende der 1960er Jahre im Auftrag der US Air Force in Zusammenarbeit zwischen dem Massachusetts Institute of Technology (MIT) und dem US-Verteidigungsministerium entwickelt wurde (Leiner et al. 2009). Im weiteren Verlauf begründete sich immer stärker die auch heute noch prägende IT-EntwicklerInnengemeinde in den USA, die das Internet als dezentralen Ort, frei von staatlicher Kontrolle und Einflussnahme als alternativen Interaktionsraum geplant hatte (vgl. Barlow 1996). Das Internet bzw. auch der Cyberspace waren somit ursprünglich ein von den USA staatlich vorangetriebenes Projekt, das in der Folge jedoch zunehmend von den daran beteiligten WissenschaftlerInnen weiterentwickelt wurde. Somit bauten die USA sowohl auf staatlicher als auch privatwirtschaftlicher Ebene ihre Kapazitäten und Fähigkeiten im ICT-Bereich erheblich aus. Gleichzeitig demonstrierten erste Vorfälle von Computerangriffen und Cyberspionage (z.B. die Spionageoperation ›The Cuckoo's Egg‹ 1986 oder der ›Morris Worm‹ von 1988) die sich bereits damals abzeichnende Verwundbarkeit von US-Systemen durch die steigende Vernetzung, was erste regulatorische Initiativen wie den ›Electronic Communications Privacy Act‹ aus 1986, den ›Computer Fraud and Abuse Act‹ aus 1986 sowie den ›Computer Security Act‹ aus 1987 zur Folge hatte (Haizler 2017, S. 33–34). Als weiterer Meilenstein in der Entwicklung der US-Cyberpolitik kann die ›Presidential Decision Directive‹ (PDD) 63 gelten, die den Schutz der amerikanischen kritischen Infrastrukturen zum Ziel hatte. Zuvor hatte die Entdeckung der bis dato ersten großangelegten und mutmaßlich durch Russland gesponserten Cyberspionage-Operation Moonlight Maze gegen US-Behörden und Forschungseinrichtungen den Handlungsdruck auf politischer Ebene entscheidend erhöht (Shackelford et al. 2017, 322, 328).

In den 1990er Jahren fokussierten sich offensive US-Cybermilitäroperationen weitgehend auf Information-Operations, wie sie in der ›Joint Doctrine for Information Operations‹ aus 1998 definiert und zuvor bereits während der Operation Desert Storm im Irak sowie im Serbien-Krieg mutmaßlich zur Anwendung kamen (Lewis 2011, S. 26): »*Information operations (IO) involve actions taken to affect adversary information and information systems while defending one's own information and information systems*« (US Joint Chiefs of Staff 1998, S. 7). Bereits 2004 bezeichnete die ›National Military Strategy‹ den Cyberspace als eine Domäne des ›Battlefields‹. Dabei gab es jedoch noch kein eigenes Cyber-Command, das erst 2009, wieder infolge einer umfangreichen russischen Cyberspionageoperation (Agent.BTZ), gegründet wurde. Zuvor hatten die Behörden der Intelligence-Community, allen voran NSA und CIA, den Cyberkonfliktaustrag der USA entscheidend geprägt und öffentlichen Quellen zufolge im Jahr 2007 die Stuxnet Operation gestartet, den bis dato disruptivsten Einsatz von Cybermitteln gegen kritische Infrastrukturen ei-

nes gegnerischen Staates (Perlroth 2021, S. 117).[118] Zudem weitete die NSA ihr globales Cyberspionage-Netzwerk in der ersten Dekade des 21. Jahrhunderts immer weiter aus, bis zumindest ein Teil hiervon durch Edward Snowden 2013 öffentlich bekannt wurde.

Die staatlichen US-Behörden verfügen somit schon seit vielen Jahren über die umfangreichsten Fähigkeiten zur Datensammlung sowie Störung fremder Systeme mithilfe von Cyberoperationen. Diese Bewertung wird durch deren erste Platzierung im NCPI sowie im Rahmen einer aktuellen, qualitativ basierten Bewertung der staatlichen Cyberfähigkeiten des International Institute for Strategic Studies (IISS) gestützt. Darin werden die USA als einzige »*Tier One-Cyber-Power*« bezeichnet (IISS 2021a).

Als militärische Cyberdoktrinen der USA sind neben der erwähnten Joint Doctrine for Information Operations die ›National Cyber Strategy‹, die ›DoD Cyber Strategy‹ sowie die J'oint Publication 3–12‹ bezüglich ›Cyberspace-Operations‹ aus 2018 zu nennen. Diese etablierten die bereits zuvor im DoD existierenden, während Trumps Präsidentschaft jedoch zunehmend zur Anwendung gebrachten Offensiv-Doktrinen ›Persistent Engagement‹ und ›Defending Forward‹.[119] Zudem begründeten sie die ›Cyber-Deterrence-Initiative‹, die kollektive Attributionen mit alliierten Partnern sowie das hierfür notwendige Teilen geheimdienstlicher Informationen vorsah (IISS 2021a, S. 16).

Wie bereits angedeutet, entwickelte sich auch im privatwirtschaftlichen Sektor der USA eine florierende IT-Branche, in der EntrepreneurInnen führender Technologie-Unternehmen wie Microsoft, IBM, Intel, Google, Apple, Facebook etc. lange Zeit das Maß aller Dinge in ihren Sektoren waren oder noch sind.[120] Aufgrund der hauptsächlich in privatem Besitz befindlichen kritischen Infrastrukturen wurde zudem früh eine Public-Private-Partnership im Cyberbereich anvisiert, die jedoch im Vergleich zur Finanzbranche als eher wenig effektiv und effizient bezeichnet wurde.[121]

Die Innovationskraft amerikanischer EntrepreneurInnen speist sich auch aus den exzellenten Lehr- und Forschungsbedingungen der nationalen Universitäten. So rangieren auch im Jahr 2020 im ›QS World University Ranking‹ im Fach ›Computer Science and Information Systems‹ auf den ersten vier Plätzen US-Universitäten, mit dem MIT an der Spitze (Top Universities 2020).

Im Gegensatz zur von Brandon Valeriano geäußerten Expertenmeinung bewertete das IISS das Ausmaß an Kooperation zwischen staatlichen und zivilen AkteurInnen im Cyberbereich als umfassend. So seien Regierung, Industrie und Wissenschaft integriert, besonders wenn es darum geht, die Geheimdienstfähigkeiten der USA zu stärken (IISS

118 Als zentrale Koordinierungsstelle fungiert das ODNI. Im Gegensatz zur CIA ist die NSA jedoch sowohl dem Verteidigungsministerium, als auch dem ODNI unterstellt.

119 Interview mit Dr. Brandon Valeriano, Mitglied der US-Cyberspace Solarium Commission, am 28.09.2020.
In einem weiteren Interview merkte Dr. Erica Borghard, ebenfalls Mitglied der Kommission an, dass die beiden Doktrinen nicht nur offensiv zu werten seien, da sie auch dazu dienen, wertvolle Informationen über das Vorgehen der Gegner zu erhalten, um somit die eigene Defensive zu stärken (Interview am 06.10.2020).

120 Insbesondere im Bereich der Consumer-Technology haben chinesische Unternehmen wie Huawei, Tencent oder ZTE in den letzten Jahren gegenüber den USA stark aufgeholt.

121 Interview mit Dr. Brandon Valeriano, am 28.09.2020.

2021a, S. 18).[122] Auch die meisten Start-ups mit großem Privatinvestment im High-Tech-Sektor werden in den USA gegründet. So war das gesamte Risikokapital-Investment der USA im Jahr 2019 dreimal so hoch wie in China und auch die US-Ausgaben für Research and Development (R & D) sind weltweit nach wie vor unübertroffen (IISS 2021a, S. 19). Der Anteil der High-Tech-Exporte am US-Gesamtexportvolumen sank jedoch über die Zeit, besonders im Vergleich zu China, was auf eine verstärkt domestische Nutzung der eigenen Innovationen oder eine stärkere Marktmacht chinesischer Unternehmen hindeuten könnte (World Bank 2021b).

Cyberkriminalität als möglicher Proxy-Pool ist für die USA aufgrund der defensiven Konzeptualisierung der IT-Unternehmen als Stellvertreter von geringerer Bedeutung und wird an dieser Stelle nicht weiter behandelt.

Tabelle 20 fasst die Ausprägungen der KV für die USA zusammen.

Tabelle 20: Die Cyber-Akteursumwelt der USA auf staatlicher/privatwirtschaftlicher Ebene

NCPI-Teilindikatoren* *(staatliche Ziele)*	Operationalisierung
Cyber Military Doctrine *(Offense)*	Joint Doctrine for Information Operations (1998) National Military Strategy (2004) National Cyber Strategy, inklusive Cyber Deterrence Initiative (2018) DoD Cyber Strategy (2018) Joint Publication 3–12 (2018)
Cyber Military Staffing/National Cyber Command *(Offense)*	*Militär* (vgl. US Cyber Command o.J.): Joint Task Force-Computer Network Defense (JTF-CND) (1998) Joint Task Force – Computer Network Operations (JTF–CNO) (1999) Joint Functional Component Command – Network Warfare (JFCC–NW) (2004) Cyber Command (2010; 2018 zum Unified Combatant Command ernannt) (NSA) *Zivile Geheimdienste:* Intelligence-Community *(ab 1981)* *Dazu zählen u.a.: (ODNI o.J.)* CIA NSA FBI Bureau of Intelligence and Research (BIR) Defense Intelligence Agency (DIA) Office of National Security Intelligence (ONSI) Private Vertragsnehmer (vgl. Shorrock 2016)

122 Dies zeigt sich auch an der CIA-gesponserten Organisation In-Q-Tel und deren Investment in Technologieunternehmen.

Global Top Technology/Cybersecurity Firms *(Offense, Commercial Gain, Intelligence)*	*U. a.* (vgl. Value 2021; Morgan 2019): Apple Microsoft Alphabet Amazon Facebook Intel Cisco FireEye Symantec CrowdStrike
High-Tech-Exports *(Offense, Commercial Gain, Intelligence)*	Relativer Anteil der High-Tech-Exporte an Gesamtexporten des Landes lag im Jahr 2007 bei ca. 30 Prozent und knapp über China. Danach sank der Anteil bis 2013 auf ca. 20 Prozent, stieg dann nochmal leicht bis 2016 an, um danach wieder zu fallen (2019: ca. 18,9 Prozent; World Bank 2021b). Der Prozentanteil der R-&-D-Ausgaben am Gesamt-BIP liegt bei den USA nach wie vor über dem Anteil Chinas, jedoch näherten sich die beiden Länder in den letzten Jahren an (World Bank 2021d).

(Eigene Darstellung)

5.6.3 Die domestischen Präferenzkonstellationen der USA und der Einfluss des allgemeinen Konfliktniveaus

Die bisherigen Ausführungen zeigen, dass sich die USA zum einen durch ihre immensen Offensivqualitäten im Cyberspace, zum anderen aufgrund ihres hohen Maßes an Digitalisierung im öffentlichen sowie privaten Sektor durch ein hohes Verwundbarkeitsniveau auszeichnen. Allein das Vorhandensein dieser Attribute reicht jedoch nicht aus, um das skizzierte Attributions- und Reaktionsverhalten der USA über die Zeit erklären zu können. Hierfür bedarf es wie im Falle der beiden Autokratien einer Analyse deren domestischer Präferenzkonstellationen auf den Ebenen des Liberalismus. Somit soll untersucht werden, inwiefern die sich durchsetzenden domestischen Interessen unterschiedlicher US-AkteurInnen das Verhalten des Landes im Cyberspace bislang prägten. Daher gilt es zunächst, die USA als Demokratie genauer zu beschreiben. Es muss darauf eingegangen werden, wie sie sich im innerdemokratischen Vergleich aufgrund ihrer institutionellen Charakteristika verorten lässt und welche Akteursgruppen daher auch über einen besonders großen Herrschaftszugang im politischen System verfügen. Dies erfolgt im Zeitverlauf für die Präsidenten George W. Bush, Barack Obama und Donald J. Trump.

5.6.3.1 Das Who's Who der amerikanischen Winning Coalition

Die USA stellen eine Präsidialdemokratie mit hauptsächlich zwei zentralen Parteien dar, über deren Stellung im Rahmen einer Mehrheitswahl entschieden wird. Im Gegensatz zum parlamentarischen System ist der US-Präsident stärker von Ad-hoc-Mehrheiten in beiden Kammern des Kongresses abhängig, gerade, wenn diese durch die Mehrheit der Mitglieder der anderen Partei dominiert werden (Lösche 2008). Seit Ende der 1990er Jah-

re kam es daher immer wieder zu einem ›Divided Government‹, da die Partei des jeweiligen Präsidenten nicht immer auch die Mehrheit im Kongress besaß.

Das Institutionenarrangement der USA zeichnet sich in erster Linie durch das Prinzip der ›Checks and Balances‹ aus: So sollen die drei Gewalten nicht nur unabhängig voneinander sein, sondern auch gegenseitige Kontrollrechte ausüben können. Beispiele wären das Veto-Recht des Präsidenten über Gesetze des Kongresses, das Recht des Supreme Courts, Gesetze des Präsidenten als verfassungswidrig zu erklären, sowie das während Donald Trumps Präsidentschaft wieder größere Aufmerksamkeit erfahrene Recht des Kongresses auf ein Amtsenthebungsverfahren des amtierenden Präsidenten (Legal Information Institute 2020). Trotz dieser strikten Trennung der Gewalten wurde bereits in den 1990er Jahren eine De-facto-Ausweitung der präsidentiellen Zuständigkeiten auf die legislativen Prozesse beobachtet (Greene 1994). Hierzu trägt aus institutioneller Sicht neben dem suspensiven Veto des Präsidenten auch die Doppelfunktion des Vizepräsidenten als gleichzeitigem Senatspräsidenten bei, der bei Stimmengleichheit letztlich die entscheidende Stimme in der Kammer hat. Im Falle einer nur knappen Senatsmehrheit der Partei des Präsidenten kann somit über das Amt des Vizepräsidenten Einfluss auf Gesetzgebungsprozesse genommen werden, wie es für die seit 2021 bestehende 50–50-Konstellation im Senat mit Kamala Harris als Vizepräsidentin öfter der Fall sein könnte (Crowley und Glueck 2021). Andersherum übt jedoch auch der Senat gewisse Machtbefugnisse auf die Exekutive aus, z.B., da dessen Zweidrittelmehrheit zur Bestätigung von Verträgen des Präsidenten mit anderen Staaten notwendig ist (US Senate o.J.).

Hinsichtlich des realpolitischen Herrschaftszugangs unterschiedlicher domestischer Akteursgruppierungen haben sich für die USA hauptsächlich vier Sichtweisen herausgebildet:

> »Majoritarian Electoral Democracy, Economic Elite Domination, and two types of interest group pluralism – Majoritarian Pluralism, in which the interests of all citizens are more or less equally represented, and Biased Pluralism.« (Gilens und Page 2014, S. 564)

Im Rahmen einer empirischen Analyse wurde für die USA der Ansatz der ›Economic Elite Domination‹ als besonders erklärungskräftig herausgestellt. Darin wird argumentiert, dass besonders AkteurInnen mit großem Ressourcenreichtum, z.B. den LeiterInnen von Großkonzernen, ein besonderer Zugang zum politischen System in den USA zukommt. Dabei können jedoch auch die Positionen einzelner AkteurInnen in politischen Institutionen oder ein gemeinsamer sozio-ökonomischer Hintergrund zu einer Interessenskonvergenz führen, die die Politik des Landes letztlich maßgeblich mitbestimmen würde (Gilens und Page 2014, S. 566). Ein Beispiel wäre die neokonservativ geprägte Policy-Elite um George W. Bush u.a. bestehend aus dem damaligen Vizepräsidenten Dick Cheney, Verteidigungsminister Donald Rumsfeld und dessen Stellvertreter Paul Wolfowitz, der ein besonderer Einfluss auf die außenpolitischen Entscheidungen Bushs attestiert wird. Deren Interessen, wie sie in der 1997 gegründeten und 2006 aufgelösten Denkfabrik »*Project for the New American Century*« (PNAC) zum Ausdruck kamen, werden somit für den Zeitraum von 2000 bis 2008 besonders relevant sein (Militarist Monitor 2019). Im Gegensatz dazu wurden unter Barack Obama im Kern noch stärker neoliberal geprägte Eliten für dessen Wirtschaftspolitik als besonders einflussreich angesehen, auch

wenn bereits unter George W. Bush persönliche Beziehungen der Politik-Eliten zur Finanzbranche sowie international agierenden Anwaltskanzleien und allgemein ›Transnational Capital‹ existierten (van Apeldoorn & Graaff 2014: 45). Zudem seien unter Bush und Obama die Verbindungen der jeweiligen Politik-Eliten zu US-Unternehmen im Allgemeinen stärker ausgeprägt gewesen als etwa zum Rüstungssektor (van Apeldoorn und Graaff 2014, S. 46)

Darüber hinaus erklärte die Studie von Giles und Page den Ansatz des ›Biased Pluralism‹ mit einem Fokus auf wirtschaftlichen Interessen von Unternehmen für die Interessensvermittlung der USA ebenfalls als erklärungskräftig. Dieser stellt zwar stärker pluralistische Interessensvermittlung in den Vordergrund, konstatiert jedoch eine Verzerrung hinsichtlich der letztlichen Interessensdurchsetzung zu Gunsten von Konzernen, unterstützt durch umfangreiches Lobbying sowie Wahlkampfspenden (Gilens und Page 2014, S. 567). Präsident Obama wurden in seinem ersten Jahr zwar erhebliche Bemühungen zur Bekämpfung dieser ungleich verteilten politischen Repräsentation attestiert, jedoch sah er sich mit erheblichen Widerständen im Senat konfrontiert. Die Interessen jener AkteurInnen, die bis dato von der dominierenden ›The-Winner-takes-it-all‹-Wirtschaft profitierten, ließen fast alle Gesetzesvorhaben scheitern, z.B. durch intensives Lobbying der US-Handelskammer im Vorfeld der Abstimmungen (Hacker und Pierson 2010, S. 8).

In der Folge wurde jedoch besonders der Einfluss des Finanzsektors sowie des neoliberal geprägten ›transnationalen Kapitals‹ auf die ökonomische Außenpolitik der Obama-Administration herausgestellt (van Apeldoorn und Graaff 2017). Im Gegensatz zur Bush-Administration war die Obama-Administration allein schon wegen der demokratischen Parteizugehörigkeit des Präsidenten weitaus progressiver und weniger konservativ geprägt. Während für Obamas Wahlsieg 2008 insbesondere US-Banken, allen voran Goldman Sachs, als Hauptsponsoren ausgemacht wurden, änderte sich deren Haltung vor der Wahl 2012, bei der sie nun den republikanischen Kandidaten Mitt Romney unterstützten. Für Obamas Wiederwahl setzten sich neben AkteurInnen der US-Unterhaltungsbranche (›Hollywood‹) besonders Unternehmen und Personen aus der Tech-Industrie (z.B. Microsoft, Google, Facebook) sowie Universitäten wie Harvard ein, indem sie als Großspender auftraten (Kotkin 2012).

Aufgrund Obamas Präferenz für einen progressiven Politikstil, in dem wissenschaftlich fundierte Fakten die Grundlage für politische Entscheidungen sein sollten, fanden sich in seiner Administration auch entsprechend viele wissenschaftliche TechnokratInnen oder WissenschaftlerInnen in beratenden Ämtern wieder. Vor allem im Umgang mit der Klimakrise verfügten progressive AkademikerInnen und NGOs über einen exponierteren Herrschaftszugang als noch zuvor unter Bush (Schambra 2009). Gleiches gilt für die zahlreichen Technologie-Firmen im Silicon Valley, denen ebenfalls ein erheblicher Zugang zu Obama persönlich und somit auch dessen Präferenzbildung bescheinigt wurde (Wortham 2016).

Donald Trump proklamierte dagegen, diesen ›Sumpf‹ in Washington, bestehend aus kapitalistischen Interessensgruppen, auszutrocknen und dem durchschnittlichen Amerikaner wieder mehr Gehör auf politischer Bühne zu verleihen. Letztlich kam es auch unter Trump zu einer Art ›Biased Pluralism‹, jedoch mit nun stärker protektionistisch statt liberal-kapitalistisch geprägten Interessensgruppen als HauptprofiteurInnen. Zu-

dem wurde die unter Obama noch stärker geförderte Technologie- und Social-Media-Branche von Trump in besonderem Maße attackiert und z.B. Google eine anti-konservative Geschäftspraxis unterstellt (Breland 2018).

Als weiterer Teil der Winning Coalition kann die Intelligence-Community gelten. Indem diese US-Präsidenten im Zuge außenpolitischer Entscheidungen auf Grundlage ihrer nachrichtendienstlichen Erkenntnisse berät, kann sie deren Entscheidungen theoretisch beeinflussen und Partikularinteressen einfließen lassen. Für die USA wurde jedoch aufgezeigt, dass geheimdienstliche Informationen im Laufe des 20. und 21. Jahrhunderts bestenfalls taktische und operative Politikentscheidungen prägen konnten, nicht aber die grundsätzlichen Leitlinien der US-Außenpolitik, da letztlich die persönlichen ›Beliefs‹ und ›Images‹ der Präsidenten und ihrer engsten BeraterInnen entscheidender waren als nachrichtendienstliche Evidenzen (Pillar 2011, S. 120).[123] Somit wird es für die weitere Analyse wichtig sein, herauszufinden, ob und wann die Geheimdienste tatsächlichen Einfluss auf inhaltliche Politikentscheidungen nehmen konnten, wann sie lediglich ihre personellen und technischen Ressourcen stärken konnten und wann deren Informationen von US-Präsidenten zur Durchsetzung der eigenen Politikpräferenzen instrumentalisiert oder manipuliert der Öffentlichkeit präsentiert wurden. In diesem Zusammenhang werden gerade für die NSA auch deren »*Institutional Birthmarks*« von besonderem Interesse sein, da das ursprüngliche Gründungsmotiv sowie die hier getroffenen ›Design-Entscheidungen‹ laut Amy Zegart die Evolution nationaler Sicherheitsbehörden umfassend prägen (Zegart 2000, S. 44). Des Weiteren können AkteurInnen der (zivilen sowie militärischen) Geheimdienstbürokratie Interessen ausbilden, die denen des Präsidenten entgegenstehen, und somit eine gewisse Non-Compliance gegenüber dessen Weisungen an den Tag legen (Zegart 2000, S. 47).[124] Dieser Aspekt wird besonders für Donald Trumps Präsidentschaft und dessen Kampagnen gegen zivile und militärische Geheimdienste als ›Deep State‹ von weiterer Bedeutung sein. Gleiches gilt für dessen anfänglich positives Verhältnis zum Militär, das er verstärkt zu parteipolitischen Verbündeten machen wollte (Brooks 2021, S. 74). Hierfür hob er u.a. Militärgeneräle in zivile Ämter, entfernte sie jedoch auch oftmals wieder zeitnah, da sie verstärkt versucht hatten, seine impulsive Außenpolitik zu moderieren (Copp 2019).[125]

Zuletzt gilt es zu bewerten, in welchen Phasen die USA stärker illiberale Tendenzen in ihrer Regierungsführung zeigten und durch welche institutionellen Prozesse dies befördert wurde. Dabei sticht Donald Trumps Präsidentschaft heraus: Auch wenn bereits unter Bush und Obama das US-System sicherlich nicht frei von Schwächen und Dysfunktionalitäten war, so konnte es dennoch als liberale Demokratie bezeichnet werden,

123 Hierzu passt auch das folgende Zitat von John Maynard Keynes: »*There is nothing a Government hates more than to be well-informed; for it makes the process of arriving at decisions much more complicated and difficult*« (zitiert in: Jervis 2017, S. 148).

124 Die Interessen führender MitarbeiterInnen staatlicher US-Behörden wurden jedoch stärker der Mitte der Gesellschaft entsprechend bewertet, als in europäischen oder asiatischen Ländern (Michaels 2017, S. 53).

125 Die letztliche Kehrtwende des Vorsitzenden des Joint Chiefs of Staff, General Miller, nachdem sich dieser von Trump für seine politischen Zwecke hatte vereinnahmen lassen, wird beschrieben in Schake 2020.

in denen die zentralen Elemente einer ›Embedded Democracy‹ hinreichend erfüllt waren. Dies änderte sich unter Trumps Präsidentschaft spürbar: Dessen Regierungsführung wurde mit der Übernahme eines Wirtschafsunternehmens verglichen. Gleichzeitig profitierten dessen Privatunternehmen von öffentlichen Aufträgen wie den zahlreichen Aufenthalten von PolitikerInnen und Behörden in Ressorts der Trump Organisation (Ford 2019).

Neben der Vermischung seines Profils als Unternehmer mit dem Amt des Präsidenten wogen Trumps Angriffe auf die Legitimität verschiedener US-Institutionen jedoch noch weitaus schwerer. Neben der bereits erwähnten Theorie eines ›Deep States‹ ließ er zahlreiche Ämter in öffentlichen Institutionen unterbesetzt und riskierte somit deren Funktionsfähigkeit (Wehle 2020). Zudem entmachtete er den Kongress de facto immer weiter (vor allem in Budgetfragen; Ip 2020), nahm Einfluss auf die künftige Zusammensetzung des Supreme Courts und unterminierte das öffentliche Vertrauen in den demokratischen Wahlprozess der USA, indem er die eigene Abwahl als Betrug am Wähler bezeichnete. Die Stürmung des Kapitols durch seine AnhängerInnen am 6. Januar 2021 stellte den vorläufigen Höhepunkt dieser Entwicklungen dar (Levitsky und Ziblatt 2018; Haberman und Martin 2021).

Diese kurzen Ausführungen zeigen bereits, dass sich die USA unter der populistisch geprägten Führung Donald Trumps immer weiter spalteten und sich dessen illiberale Handlungen auch auf institutioneller Ebene spürbar machten. Zudem vertieften sich die Konfliktlinien zwischen den Parteien, aber auch innerhalb der Republikanischen Partei immer weiter. Dieser Wandel hin zu einer stärker populistisch-illiberalen Form der Demokratie wird somit für die Analyse des Untersuchungszeitraums während der Trump-Präsidentschaft besonders bedeutend sein.

5.6.3.2 George W. Bush und sein neokonservativer Beraterkreis

> »They [die Neokonservativen; Anm. der Autorin] seem to have captured the heart and mind of the President, and they're controlling the foreign policy agenda.«
> *Joe Biden 2003, zitiert in Daalder und Lindsay (2003, S. 15)*

Zu Beginn der Analyse stehen die Präferenzkonstellationen von George W. Bush und dessen neokonservativem Beraterkreis (2000–2008) im Fokus. Hierzu zählen in erster Linie der damalige Vizepräsident Dick Cheney, der Verteidigungsminister Donald Rumsfeld sowie dessen Stellvertreter Paul Wolfowitz. Diesem Teil der Winning Coalition wird ein erheblicher Einfluss auf die staatliche Präferenzbildung auf außenpolitischer Ebene attestiert, die im Zuge des nach 9/11 gestarteten NSA-Überwachungsprogramms jedoch auch Auswirkungen auf die domestische Ebene hatte.

Auch wenn der amerikanische Neokonservatismus seine Ursprünge bereits in den 1930er Jahren hatte und dessen selbsternannter ›Pate‹, Irving Kristol, in dieser Anfangsphase mit Ideen des Trotzkismus sympathisierte (Ross 2005, S. 16), erfolgt die Auseinandersetzung in diesem Abschnitt ausschließlich mit den Interessen der zweiten Generation der US-Neokonservativen nach dem Ende des Kalten Krieges. Dabei wird untersucht, inwiefern diese die Befunde des HD-CY.CON für die USA vor 2009 erklären können. Hierbei stehen notwendigerweise stärker die offensiven Cyberaktivitäten der USA im Fokus der Erklärung, da es für die konzeptualisierte Staat-Proxy-Beziehung im

Rahmen der Attributionsprozesse privater IT-Unternehmen in diesem Zeitraum kaum Anhaltspunkte im HD-CY.CON gibt. Da Letztere jedoch in dieser Arbeit auch als Produkt der eigenen Offensivoperationen im Cyberspace angesehen werden, hat dieser Abschnitt auch für die spätere Analyse defensiver US-Cyberproxys seine Bedeutung.

Sicherheit durch Abschreckung nach 9/11

Bereits in den 1980er Jahren etablierte sich in den USA das Narrativ von sog. ›Rogue States‹, also ›Schurkenstaaten‹, die erstens gegen internationale Menschenrechte auf heimischem Boden verstoßen, zweitens Terrorgruppen unterstützen und drittens nach Massenvernichtungswaffen streben (Homolar 2011, S. 710). Nach dem Ende des Kalten Krieges verstärkte sich die Unsicherheit der USA, von welcher Seite aus nun anstelle der UdSSR die stärkste Gefahr drohe. Als der Irak unter Saddam Hussein im Jahr 1990 in Kuwait einfiel, nahm die neokonservative Politik-Elite in den USA dies zum Anlass, das Saddam-Regime zum bedrohlichen Schurkenstaat zu erklären, nachdem zuvor jahrelang in der Region miteinander kooperiert wurde (Dumbrell 2018).

Aus Sicht der damaligen US-Neokonservativen waren die USA als militärisch und moralischer Hegemon und nach dem Sieg über die Sowjetunion als einziges Land in der Lage, für Frieden und Stabilität zu sorgen. Zur Durchsetzung dieser moralischen Überlegenheit sei zudem militärische Gewaltanwendung notwendig. Für die auch vom neokonservativen Think Tank ›Project for the New American Century‹ bereits im Jahr 2000 geforderten Präemptiveinsätze gegen Länder wie den Irak mangelte es vor 9/11 jedoch an einer entsprechenden Sicherheitsbedrohung (vgl. Shah 2004). Als legitimationstheoretischer Ausgleich wurde daher besonders für den 2003 initiierten Irakkrieg das Narrativ der ›Democracy-Promotion‹ gepflegt (Carothers 2007, S. 5). Dies erschien besonders notwendig, nachdem öffentlich eingestanden werden musste, dass der Irak offensichtlich nie über Massenvernichtungswaffen verfügt hatte. Die Vorstellung der USA als ›Befreier des irakischen Volkes‹ entspricht zudem den ideellen Interessen der neokonservativen Eliten nach einer stärker christlich-religiös geprägten Außenpolitik. George W. Bush brachte dies mit seiner Äußerung zum Ausdruck, er sei »*von Gott beauftragt*« worden, den Irak von der Saddam-Diktatur zu befreien (übersetzt in: MacAskill 2005).

Auf außenpolitischer Ebene führte der exponierte Herrschaftszugang der neokonservativen Eliten um Bush dazu, dass diese ihn nicht nur infolge von 9/11 zur breit unterstützten Militärkampagne in Afghanistan gegen Al-Quaida, sondern zwei Jahre später auch zum Militärschlag gegen Saddam Hussein bewegen konnten. Hierdurch sollte die exponierte militärische Abschreckungsfähigkeit der USA infolge des 9/11-Schocks wiederhergestellt werden (Butt 2019). Jedoch teilte Präsident Bush bereits das grundlegende Interesse nach einem militärischen Vorgehen gegen Saddam Hussein, um das unter seinem Vater begonnene Militärvorgehen gegen den irakischen Diktator abzuschließen (Al-qatari und Gambrell 2018).

Durch das immense Militärengagement der USA im Nahen Osten seit 9/11 und bis zur Präsidentschaft Obamas lassen sich vor allem zwei der gegen US-Ziele gerichteten Cyberoperationen vor 2009 erklären: Die russische Spionageoperation Agent.BTZ im Jahr 2008 sowie die ›Operation Mermaid‹ der als iranischer Proxy attribuierten APT ›Infy‹ im Jahr 2007 (Bar und Conant 2016). Erstere erfolgte, wie bereits beschrieben, durch eine Überwindung der Air-Gap-Systeme des US-Militärs, indem auf einem US-Stützpunkt

der USA im Nahen Osten ein infizierter USB-Stick abgelegt wurde. Wie im Kapitel zu Russland aufgezeigt, existierten in der amerikanisch-russischen Beziehung zu dieser Zeit erhebliche Spannungen, laut Putin auf der Münchner Sicherheitskonferenz 2007 ausgelöst aufgrund der amerikanischen Militärpolitik in der Region. Russische Cyberoperationen dienten somit bereits in dieser Frühphase des Cyberkonfliktaustrags der Manipulation von Verwundbarkeiten, in diesem Fall der USA, auf militärpolitischer Ebene. Demgegenüber richtete sich die iranische Cyberspionageoperation ›Mermaid‹ außer gegen die USA auch gegen politische Ziele in Dänemark und Israel (360Helios 2016). Dänemark war offizieller Bestandteil der ›Koalition der Willingen‹ im Irak, einem direkten Nachbarn des Iran. Israel wurde zudem zumindest inoffiziell immer wieder ein großes Interesse am US-Vorgehen gegen das Saddam-Regime sowie Teheran attestiert (Waxman 2009). An dieser Stelle angemerkt sei jedoch, dass bis 2009 zahlenmäßig chinesische Cyberspionageoperationen gegen US-Ziele das Bild im HD-CY.CON dominierten. Dies lässt sich auf die auch unter Bush dominierenden Wirtschaftspräferenzen einer neoliberalen Agenda mit freiem Marktzugang im Rahmen der ›Open-Door‹-Policy sowie die zunehmende Verwundbarkeit der US-Unternehmen im Cyberspace zurückzuführen (vgl. van Apeldoorn und Graaff 2014, S. 35).[126]

Neben der expansiv-militärischen Außenpolitik der USA, die sie für Cyberspionageoperationen politischer Kontrahenten besonders attraktiv werden ließ, erklären die Afghanistan- und Irakkriege bzw. deren Einbettung in den ausgerufenen ›War on Terror‹ auch die immensen eigenen Cyberspionageaktivitäten der USA in der Frühphase des HD-CY.CON. Die Ausführungen der New-York-Times-Reporterin Nicole Perlroth in ihrem Buch aus 2021 veranschaulichen das unvergleichliche Ausmaß, mit dem die NSA im Laufe der Jahrzehnte ihre Kompetenzen und Befugnisse im Bereich der SIGINT sowie durch das Ausnutzen von Exploits unterstützter Cyberspionage sukzessive ausweitete. Infolge von 9/11 erhielten deren Interessen an noch mehr Überwachungsbefugnissen einen entscheidenden Antrieb, was zur von Edward Snowden 2013 offengelegten weltweiten US-Überwachungsinfrastruktur führte (vgl. Snowden 2019).

Auf der Offensivseite setzten sich somit inhaltlich die neokonservativen Eliten mit ihrem Bestreben nach Sicherheit durch Abschreckung durch, die primär durch den Irakkrieg sowie die Überwachung einheimischer und ausländischer Ziele und somit auch befreundeter Staaten etabliert werden sollte. Auch wenn die geheimdienstlichen Informationen in Teilen seitens der Bush-Administration während der Irakkriegsentscheidung ignoriert bzw. öffentlich auch bewusst falsch dargestellt wurden (Betts 2007, S. 597), bot eben diese militärische Expansionspolitik jenen Geheimdiensten ein ›Window of Opportunity‹, um die eigenen bürokratischen Interessen weiter verfolgen zu können.

Im HD-CY.CON drückt sich diese Obsession für die Sammlung von nachrichtendienstlichen Informationen in den 13 verzeichneten Spionageoperationen der USA zwischen 2001 und 2008 aus, für die zehnmal die NSA[127] sowie zweimal die CIA verantwortlich gemacht wurden. Hierzu ist allerdings anzumerken, dass dabei oftmals wohl

126 Die ›Open Door‹-Policy kann durch folgende Elemente beschrieben werden: Ökonomische Expansion, Förderung freier Märkte, eine liberale Weltordnung sowie Demokratieförderung (van Apeldoorn und Graaff 2014, S. 35).

127 In zwei Fällen in Kooperation mit dem britischen GCHQ.

tausende Infiltrationen unter einer Kampagne zusammengefasst wurden und alternative Falldefinitionen sicherlich zu einer noch weitaus größeren Anzahl führen würden. In acht der 13 Fällen wurden direkt politische AkteurInnen und Institutionen mit weltweiter Verteilung anvisiert. Zudem wurden IOs wie die UN zu Spionageopfern, aber auch das internationale Zahlungssystem SWIFT wurde ausspioniert, um den Geldfluss mutmaßlicher TerroristInnen überwachen zu können (Poitras et al. 2013). Die USA nutzten somit an dieser Stelle ihren exponierten Zugang zu international verteilten Hard- und Software-Systemen aus und nahmen dabei weitgehend keine Rücksicht auf bestehende Interdependenzbeziehungen zu alliierten Staaten. Das gemeinsame Interesse an geheimdienstlichem Austausch sollte für diese aus Sicht der USA die Kosten des ›Ausspähens unter Freunden‹ überwiegen (EURACTIV 2017).

Nicht nur Cyberspionageoperationen, sondern auch die bis dato bekannteste Cybersabotage-Operation der bisherigen Geschichte fällt in ihrem Ursprung in die Präsidentschaft Bushs. So forderte dieser bereits im Juni 2007 eine ›dritte Option‹ im Umgang mit dem Iran. Zuvor hatte sich der Druck Israels auf die US-Administration massiv erhöht, da Israel zu einem Militärschlag gegen Teheran drängte, um dessen Nuklearwaffenprogramm zu unterbinden. Sämtliche diplomatische Versuche, den Konflikt zu befrieden, hatten zuvor als Option 1 keinen Erfolg gebracht (Perlroth 2021, S. 117). An dieser Stelle kam ferner die zu diesem Zeitpunkt dominante Stellung der NSA in außenpolitischen Fragen zum Ausdruck, da deren Vorschlag zur Umsetzung von Stuxnet tatsächlich angenommen wurde.

Diese Hinwendung zu weniger gewaltsamen Konfliktmitteln unter Bush könnte als Ausdruck des sich zu diesem Zeitpunkt bereits abgezeichneten Misserfolges der militärischen Invasionspolitik im Nahen Osten gewertet werden. So schoben direkt an der Kriegsentscheidung beteiligte Neokonservative Präsident Bush zunehmend die alleinige Schuld für das Scheitern des Projektes »*Iraqi Freedom*« zu, während Neokonservative der ersten Generation Verrat an der neokonservativen Leitidee »*of using our power for moral good in the world*« beklagten (Kenneth Adelman, zitiert in: Borger 2006). Die neokonservative Überzeugung der militärischen Überlegenheit der USA hatte im Zuge des Irakkrieges gelitten, asymmetrischer Konfliktaustrag etablierte sich immer mehr als profundes Gegenmittel (Locks 2015). Somit könnte die vom damaligen NSA-Direktor Keith Alexander versprochene gewaltlose Lösung des ›Iran-Problems‹ auch eine attraktive Option für Bush dargestellt haben, um durch eine allgemeine Konflikteskalation mit dem Iran die oftmals als ›Pulverfass‹ beschriebene Region nicht endgültig zum Explodieren zu bringen. Die Konfliktverläufe in Afghanistan, besonders jedoch dem Irak, hatten den USA ihre auch auf konventioneller Ebene bestehende Verwundbarkeit gegenüber asymmetrischem Konfliktaustrag vor Augen geführt. Da gleichzeitig mit Israel eine sicherheitspolitische Interdependenzbeziehung bestand und dieses ein aggressiveres Vorgehen gegen den Iran forderte, waren die USA an einem deeskalativeren Konfliktmittel mehr als interessiert, um die eigene Verwundbarkeit nicht noch größer werden zu lassen. Zwischen 2000 und 2008 (Attributionsjahre) wurden im HD-CY.CON lediglich vier Attributionen von US-IT-Unternehmen registriert, was jedoch dem damaligen Entwicklungsstadium der Branche entspricht. In zwei der vier Fällen nahmen auch politische AkteurInnen aus den USA eine Attribution vor, jedoch ausschließlich in Form von anonymen Zitaten in Medienberichten. Des Weiteren wurden in zwei von vier Fällen die technischen Attribu-

tionen im Rahmen der Medienberichterstattung veröffentlicht und nicht in Form von umfangreichen Berichten, die sich erst ab 2014 stärker etablierten. In einem Fall von vier Fällen fand die technische Attribution erst nach der politischen Attribution und im Jahr 2009 statt:[128] Hierbei handelte es sich um den im März veröffentlichten Bericht der selbsternannten Open-Source-Initiative ›Grey Goose‹. Da dieses Projekt jedoch bereits 2008 mit dem Ziel der Analyse einer potenziellen russischen Beteiligung an den DDoS-Operationen gegen georgische Ziele gegründet wurde, wird es in diesem Abschnitt behandelt. Der entsprechende Bericht ist ein frühes Beispiel für umfassendere, technische Beweisführung zur Analyse und in diesem Falle auch Attribution von Cyberoperationen. Darin wird zudem auf eine mögliche Involvierung des GRU hingewiesen sowie die Verantwortlichkeit der Nashi-Jugendgruppe als russischer Proxy thematisiert (Grey Goose 2009). Da GreyLogic als IT-Unternehmen erst aus Grey Goose hervorgegangen ist und zudem keine US-Ziele betroffen waren, wird dieser Fall jedoch auch nicht als Vorgang im Rahmen einer defensiven Staat-Proxy-Beziehung behandelt.

Insgesamt etablierte sich die USA unter Präsident Bush als auch im Cyberspace hegemonial auftretender Akteur, der bereit ist, seine Interessen auch auf Kosten alliierter Staaten durchzusetzen, wie im Zuge der NSA-Affäre deutlich wurde. Deren allgemeine Interessenkonvergenz führte bei diesen zu keinem signifikanten Widerstand, zu groß war und ist die Abhängigkeit von den USA aus sicherheitspolitischer Sicht. Gleichzeitig demonstrierten die US-Geheimdienste mit ihrer Stuxnet-Operation jedoch auch erstmals das disruptive Potenzial offensiver Cyberoperationen und öffneten aus Sicht von ExpertInnen somit gewissermaßen die ›Büchse der Pandora‹ gegenüber weniger von den USA abhängigen Autokratien (Kuhn 2010).

Im nachfolgenden Abschnitt stehen die Interessen der dominanten Teile der Winning Coalition unter Präsident Obama im Fokus. Es wird der Frage nachgegangen, wie sie die in dieser Phase initiierten Attributionen seitens US-IT-Unternehmen erklären können.

5.6.3.3 Die USA unter Barack Obama als ›Cyber-Ziel‹ Nr. 1

> »So cyberspace is real. And so are the risks that come with it. It's the great irony of our Information Age – the very technologies that empower us to create and to build also empower those who would disrupt and destroy.«
> *Barack Obama 2009, in The White House (2009a).*

Das voranstehende Zitat verdeutlicht, wie sich die USA speziell während der Präsidentschaft Barack Obamas ab 2009 immer weiter zum am stärksten von Cyberoperationen betroffenen Land entwickelten. Infolge der Offenlegung von Stuxnet 2010 sowie der Snowden-Enthüllungen 2013 verstärkten Staaten wie China, Russland, Iran oder Nordkorea ihre eigenen Cyberaktivitäten oder bauten erst eigene Kapazitäten auf.

Für die republikanische Ebene sind während der Obama-Präsidentschaft besonders folgende Aspekte relevant: Die Verwendung von privaten Unternehmen als Vertragsnehmern und somit potenziellen offensiven Cyberproxys ist seit 2009 durch die Intelligence-

128 Die Angabe 2008 als Attributionsjahr bezieht sich somit in diesem Fall auf die politische Attribution.

Community Directive (ICD) 612 des ODNI geregelt. Diese verbietet besonders die Ausübung von »*inherently governmental activities*« durch private Vertragsnehmer (Halchin 2015, S. 15). Dass hierunter auch die finale Ausführung von Cyberoperationen fällt, sei es zu Spionage- oder Sabotagezwecken, erscheint plausibel. Somit ist auf institutioneller Ebene der Gebrauch offensiver Cyberproxys in den USA de jure verboten. Bereits der ›Computer Fraud and Abuse Act‹ von 1984 hatte der US-Regierung erhebliche Beschränkungen bezüglich einer potenziellen Auslagerung offensiver Cyberoperationen an US-BürgerInnen auferlegt (Farwell & Rohozinski 2011: 36). Infolge der Snowden-Enthüllungen erfuhr jedoch die de facto-Ausgestaltung der Beziehung zwischen der Intelligence-Community und den Vertragsnehmern auch auf politischer Ebene in den USA vermehrte Aufmerksamkeit:

> »First and foremost, an agency that turns over too much responsibility to contractors runs the risk of hollowing itself out and creating a weaker organization. The agency could also lose control over activities and decisions that should lie with the government, not with contractors.« Thomas Carper, Vorsitzender des Senate Select Committee on Intelligence, am 18. Juni 2014, zitiert in: Halchin (2015, S. 2)

Die im Rahmen der ICD 612 vorgeschriebenen Berichtspflichten der Intelligence-Community über das Ausmaß und die Art der Anstellung welcher Vertragsnehmer wurden laut BeobachterInnen unterschiedlich erfüllt. Zudem sei zu diesem Zeitpunkt unklar gewesen, wie genau die verschiedenen Behörden ihre Compliance mit der ICD 162 sicherstellen (wollen) (Halchin 2015, S. 15).[129] Nichtsdestotrotz weisen die ICD 612 sowie die während der Obama-Präsidentschaft angestrebten Post-Snowden-Bemühungen verschiedener US-Instanzen nach größerer Kontrolle der Geheimdienste auf eine Einhegung derer Interessensdurchsetzungschancen zumindest aus rechtlicher Sicht hin. Auch die unter Obama implementierte Position eines nationalen ›Cyber-Security-Coordinator‹ ist ein Indiz für eine zu diesem Zeitpunkt stärker zentralisierte Koordination und Kontrolle der geheimdienstlichen Tätigkeiten im Cyberspace (The White House 2009b). Inwiefern Donald Trump den Entscheidungsprozess im Rahmen offensiver Cyberoperationen der USA wieder stärker dezentralisierte und besonders dem US CYCOM größere Handlungsautonomie einräumte, wird im nachfolgenden Abschnitt behandelt.

Die Analyse der ideellen sowie wirtschaftlichen Interessen der Obama-Administration erfolgt anhand ausgewählter Attributionssequenzen, um den Zusammenhang zwischen UV und AV eindeutiger fassen zu können: Es handelt sich um den APT1-Bericht und die darauffolgende Anklageerhebung aus 2014 sowie den DNC-Hack aus 2016. Die Interessen der während der Obama-Präsidentschaft besonders einflussreichen Interessensgruppen werden somit zu diesen konkreten Attributionsfällen direkt in Bezug gesetzt. Es wird nicht behauptet, dass hiermit die gesamte Breite der erfassten US-Attributionspraktiken abgedeckt werden kann. Dennoch stellen diese beiden Fälle sinnvolle Anknüpfungspunkte für die Analyse des Einflusses der UV auf die AV unter Obama dar,

129 Im Rahmen einer 2014 abgehaltenen Anhörung des Homeland Security & Governmental Affairs Committee wurde die unterschiedliche Bewertung der Art und des Ausmaßes der Kontrolle der Behörden über ihre Vertragsnehmer deutlich (Halchin 2015, S. 16–17).

da hierbei (wie in 5.6.1 aufgezeigt) die konzeptualisierte defensive Staat-Proxy-Beziehung auch am ehesten plausibilisiert werden konnte.

Der APT1-Bericht und die PLA-Anklage: Transnationale US-Unternehmen und der Diebstahl geistigen Eigentums

Die bereits unter George W. Bush stetig gestiegene Cyberspionage mutmaßlich chinesischer AkteurInnen gegen US-Unternehmen erreichte zu Beginn der zweiten Amtszeit Barack Obamas neue Dimensionen:[130] So schätzte die ›Commission on the Theft of American Intellectual Property‹ im Jahr 2013 den ungefähren jährlichen Schaden, der US-Unternehmen durch chinesischen Diebstahl geistigen Eigentums zu dieser Zeit entstand, auf ca. 300 Milliarden US-Dollar. Politisches Handeln sei daher endlich zwingend erforderlich, da Cybersicherheitsmaßnahmen allein nicht ausreichen würden (Corbin 2013).

Das Interesse vieler US-Unternehmen nach verstärkten Maßnahmen der Regierung gegen ökonomisch motivierte Spionage spiegelt sich auch in den Daten des HD-CY.CON wider: So wurden allein in den Jahren 2009 bis 2011 18 Cyberspionageoperationen staatlicher oder staatlich gesponserter AkteurInnen verzeichnet, in denen US-Unternehmen, aber auch Finanzinstitute oder Rüstungsunternehmen sowie weitere Teile kritischer Infrastrukturen, als Ziele erfasst wurden. Die Brisanz und stetige Zunahme chinesischer Cyberspionageoperationen gegen US-Ziele führten somit zu verstärktem Druck seitens US-Geschäftsgruppierungen auf die Administration, speziell im Vorfeld des Obama-Xi-Gipfels (King & Spalding 2015).

Diese zeitlichen Abläufe korrespondieren mit dem aufgezeigten Anstieg privatwirtschaftlicher Attributionen seitens US-IT-Unternehmen ab 2013. Zwar hatte es bereits 2010 infolge des Bekanntwerdens der chinesischen Cyberspionageoperation Aurora gegen Google einen technischen Bericht von McAfee gegeben. Die Attribution in Richtung Peking wurde damals jedoch nicht durch das IT-Unternehmen, sondern durch Google selbst vorgenommen. In der Folge blieben die politischen Reaktionen auf US-Seite zumindest in der Öffentlichkeit verhalten. Als Erklärung, warum Operation Aurora dennoch nicht als ›First Encounter‹ der konzeptualisierten defensiven Cyberproxy-Beziehung im Falle der USA gelten kann, wird die erst danach hinreichend erfolgte Weiterentwicklung der technischen Attributionsfähigkeiten der US-IT-Unternehmen angeführt (Clayton 2012). Indem ab 2013 IT-Unternehmen wie Mandiant zunehmend Angriffsdetails veröffentlichten, trugen diese direkt zur Resilienzstärkung der anvisierten Ziele bei.

---

130 Den Anfang machen die kommerziellen Interessen jener US-Unternehmen, die transnational operieren und aufgrund der Bedeutung geistigen Eigentums für ihr Geschäftsmodell durch Spionage jeglicher Art mit erheblichen Einbußen zu rechnen haben. Somit werden hier Banken, Rüstungskonzerne, Software-Unternehmen oder auch Ingenieursbüros als relevanter erachtet, als etwa Landwirtschaftsunternehmen, die durch Exportgeschäfte ebenfalls transnational, jedoch (zumeist) weniger innovationsgetrieben agieren. Natürlich können auch Unternehmen der Lebensmittelbranche über sensible Daten verfügen, z.B. Kundendaten, Geschäftsgeheimnisse, aber auch z.B. im Falle gentechnisch manipulierter Produkte wissenschaftliche Daten. Die Wahrscheinlichkeit eines solchen Datendiebstahls wird für diese jedoch gemeinhin als geringer eingeschätzt, als etwa die Gefahr durch Ransomware-Operationen, wie sie 2021 gegen den größten Fleischproduzenten der Welt, JBS, eingesetzt wurden (Mccrimmon und Matishak 2021).

Das aufgezeigte Investment von In-Q-Tel in diverse US-IT-Unternehmen kann also besonders durch das gesteigerte Interesse der Obama-Administration an besserem Schutz vor immer umfassenderen chinesischen Cyberspionageakten erklärt werden.

Gleichzeitig legen die 2013 durch Mandiant erstmals veröffentlichten Attributionsevidenzen nahe, dass nicht nur technische Resilienz, sondern auch eine Signaling-Wirkung hiermit intendiert gewesen ist. Indem Mandiant bereits 2013 China erstmals öffentlich der Cyberspionage ›überführte‹, wusste die chinesische Gegenseite, dass Attribution sehr wohl möglich ist. Wie seitens der ›Commission on the Theft of American Intellectual Property‹ gefordert, arbeitete die US-Regierung jedoch zu diesem Zeitpunkt wohl bereits in Form der 2014 erfolgten Anklageerhebung gegen PLA-Angehörige an einer politischen Reaktion. Als Grund hierfür kann der aufgezeigte Druck wirtschaftlicher AkteurInnen auf die US-Regierung nach der Veröffentlichung des APT1-Berichtes durch Mandiant genannt werden. So erfüllte dieser zwar eine Resilienz- sowie eine Signaling-Wirkung, setzte die Administration jedoch in der Folge auch unter verstärkten Handlungsdruck. Diesem kam die Regierung in Form der ersten Anklageerhebung gegen ausländische Hacker 2014 nach.

In Kombination mit dem Erlass sowie der Androhung weiterer Wirtschaftssanktionen gelang es der Obama-Administration, die Interessen der heimischen Wirtschaft in politische Maßnahmen umzusetzen. Die damals bestandenen wirtschaftlichen Interdependenzen der beiden Länder, gepaart mit einem beidseitigen Interesse an möglichst freiem Handel, können somit das Zustandekommen des Cyberabkommens erklären. Die legitimatorische Grundlage hierfür hatten jedoch der Mandiant-Bericht sowie die nachgelagerte Anklageerhebung gelegt, auch mit dem Vorteil eines jeweiligen ›First-Encounter‹-Moments. Theoretisch gesprochen schuf somit die öffentliche Attribution des defensiven Cyberproxys (Mandiant) die Grundlage für die nachgelagerte politische Attribution und Reaktion, die wiederum auf die Manipulation der bestehenden Verwundbarkeitsasymmetrie gegenüber China abzielten. Dass dieses Abkommen zumindest zeitweilig ein Erfolg war, wurde von IT-Experten bestätigt (Segal 2016). Dessen Nichteinhaltung durch China ab 2017 kann auf eine veränderte Interdependenzbeziehung der beiden Länder auf wirtschaftlicher Ebene zurückgeführt werden, die im Abschnitt zur Trump-Administration näher behandelt wird.

Im Gegensatz dazu verdeutlicht die vergleichbare Passivität der Obama-Regierung infolge des OPM-Hacks 2015, dass es sich hierbei um politische Spionage handelte, die sich die USA auch infolge der NSA-Affäre weiterhin offenhalten wollten. Eine politische Attribution und politische Gegenreaktion lagen hier somit weniger im Interesse der Administration. Nichtsdestotrotz hatten »*Senior American Officials*« im Juli 2014 das Stattfinden des ersten Hacks selbst öffentlich gemacht, indem sie die Information an die New York Times geleakt hatten (Schmidt et al. 2014). Der OPM-Hack könnte somit ein Beispiel dafür sein, wie innerhalb einer Demokratie unterschiedliche AkteurInnen im Rahmen eines Attributions- und Reaktionsprozesses Druck aufeinander ausüben: So war nicht jeder im politischen System von der Effizienz der Anklage aus 2014 überzeugt. Der OPM-Hack als Akt der politischen Spionage führte jedoch wohl auch deshalb zu keiner offiziellen US-Attribution, da parallel durch das Obama-Xi-Abkommen der ›eigentliche Problemfall‹ der Wirtschaftsspionage zumindest vorläufig adressiert werden konnte.

CrowdStrike und der DNC-Hack: Die US-Demokratie in Zeiten starker Polarisierung
Drei Aspekte spielten für die zögerliche US-Reaktion während der russischen Wahlbeeinflussung 2016 eine Rolle:

1. Die Verletzlichkeit der US-Demokratie in Zeiten stark polarisierter Wahlen;
2. die Verletzlichkeit der US-Demokratie gegenüber russischen Eskalationen sowie
3. die Interessen unterschiedlicher Teile des politischen Systems (State Department und Pentagon vs. Intelligence-Community).

Als die republikanische Partei Donald Trump im Juli 2016 offiziell zu ihrem Präsidentschaftskandidaten erklärte, befanden sich die USA bereits in einem andauernden Prozess der zunehmenden gesellschaftlichen und parteipolitischen Polarisierung. Letztere ist in Zeiten nationaler Wahlen generell erhöht, jedoch erreichten die rhetorischen Anfeindungen des Trump-Lagers in Richtung der demokratischen Gegenseite bereits vor dessen Ernennung neue Ausmaße. Die öffentliche Russland-Attribution von CrowdStrike im Juni 2016 brachte die Obama-Administration daher trotz ihrer Signaling-Funktion in eine schwierige Situation: Einerseits erforderte die Integrität der Präsidentschaftswahl ein entschlossenes Benennen russischer Verantwortlichkeiten, andererseits wollte Obama den Vorwurf einer politischen Einflussnahme in die Wahlen vermeiden, indem Russland der Wahlbeeinflussung zu Gunsten Donald Trumps beschuldigt wurde. Auch wenn Studien zufolge die gesellschaftliche Polarisierung bereits während Barack Obamas Präsidentschaft stetig zugenommen hatte (Schreyer 2017), wollte dieser doch stets als vereinigender Präsident wahrgenommen werden, der keine Gruppierungen gegeneinander ausspielt.[131] Genau diesen Ansatz verfolgte jedoch Donald Trump seit der Bekanntgabe seiner Kandidatur, indem er sich quasi als Befreier der ›entrechteten‹ Amerikaner, vor allem des ›Rust Belts‹, darstellte, der konsequent gegen die korrupten Politik- und Wirtschaftseliten in Washington vorgehen würde (vgl. Kastein 2020). Trump behauptete zudem bereits lange vor der Wahl, dass das Establishment diese fälschen würde (Diamond 2016). Wohl auch, um dieser Behauptung keine weitere Nahrung zu liefern, entschied sich Obama dazu, bis einen Monat vor der Wahl mit einer politischen Attribution zu warten. Dass er diese jedoch nicht selbst präsentierte, kann als weiteres Indiz dafür gewertet werden, dass Obama eine Politisierung der Attribution hierdurch vermeiden wollte (Huetteman 2017). Diese sah er offensichtlich als unvermeidlich an, hatte doch das populistische Auftreten Trumps und seiner AnhängerInnenschaft zu einer immer stärkeren parteipolitischen Spaltung der USA geführt. Obwohl Trump zu diesem Zeitpunkt noch kein gewähltes Mitglied des politischen Systems war, hatte er sich jedoch vor allem über Social Media einen erheblichen Einfluss auf die ideellen Interessen weiter Teile der Bevölkerung und durch die bevorstehenden Wahlen somit gewissermaßen auch bereits einen gewissen Herrschaftszugang gesichert. Somit erklärte er die US-Wahlen zu einem Nullsummenspiel,

---

131 »*By ourselves, this change will not happen. Divided, we are bound to fail.* […] *beneath all the differences of race and region, faith and station, we are one people.*« (Barack Obama auf einer Wahlkampfveranstaltung 2007, zitiert in: The Guardian 2007).

in dem konziliante Sichtweisen zwischen den immer konfliktiveren Präferenzen der beiden Seiten kaum noch Raum fanden.

Als zweiter Aspekt der US-Reaktion auf den DNC-Hack kann die wahrgenommene Verwundbarkeitsasymmetrie gegenüber Russland genannt werden. Mittlerweile ist bekannt, dass die US-Regierung bereits seit 2014 von Geheimdiensten gewarnt wurde, dass Russland seine Beeinflussungsmaßnahmen weltweit intensiviert hatte und auch gegen die USA einsetzen würde (Watkins 2017). Das zögerliche Vorgehen der Obama-Administration, erst einen Monat vor der Wahl Russland der Wahlbeeinflussung zu beschuldigen, kann somit auch durch die wahrgenommenen Verwundbarkeitsasymmetrien zwischen den beiden Ländern erklärt werden. Obwohl die Geheimdienste Obama diverse Beantwortungsoptionen bereits im Sommer 2016 vorgelegt hatten, entschied er sich vor der Wahl zu keiner politischen Reaktion. Ausschlaggebend war die Angst, Russland hierdurch zu einer weiteren Eskalation zu provozieren, die die USA aufgrund der eigenen Verwundbarkeiten während Wahlen ungleich schwerer getroffen hätten (Watkins 2017).

Als dritten Teilaspekt der Obama-Reaktion können die teils gegensätzlichen Interessen des State Departments und des Pentagons auf der einen sowie der Intelligence-Community auf der anderen Seite genannt werden. Da sich die beiden erstgenannten Akteure stärker in der Schusslinie möglicher Gegenreaktionen Russlands sahen als die zumeist verdeckt agierende Geheimdienstcommunity, schreckten diese auch vor entschlossenen Gegenmaßnahmen eher zurück (Watkins 2017). Unabhängig von einer möglichen Gegenmaßnahme urteilte der damalige Heimatschutzminister bei einer Anhörung im Repräsentantenhaus 2017, dass die Regierung zudem das Offenlegen geheimdienstlicher Methoden im Rahmen einer politischen Attribution vermeiden wollte. Diese beiden Aspekte könnten somit als Gegensätze verstanden werden: Einerseits votierte die Geheimdienstcommunity für entschlossenere Gegenmaßnahmen, andererseits wollte sie ihre eigenen Methoden im Rahmen einer Attribution nicht zu umfassend offenlegen. Eine Schlussfolgerung hieraus könnte jedoch sein, dass besagte Gegenmaßnahmen wohl hätten verdeckt stattfinden sollen, wofür eine öffentliche Attribution nicht notwendig bzw. sogar kontraproduktiv gewesen wäre.

Im Gegensatz zur APT1-Attribution durch Mandiant gab es somit im Falle des DNC-Hacks keine eindeutig zu identifizierende Interessensgruppe, die als primär ausschlaggebend für das Verhalten der Obama-Administration hätte gewertet werden können. Im Gegensatz zur chinesischen Wirtschaftsspionage herrschte 2016 kein überparteilicher Konsens vor, dass Russland als Bedrohung für die US-Demokratie zu werten sei. Ursächlich hierfür waren die zunehmende Parteipolarisierung sowie der sich bereits im Wahlkampf abzeichnende, illiberale Führungsstil Donald Trumps. Stattdessen sah sich Obama mit einer Vielzahl an konträren Interessenlagen konfrontiert, die er durch eine verspätete sowie abgeschwächte öffentliche Attribution abzumildern versuchte. Indem infolge des DNC-Hacks keine zeitnahe Gegenkommunikation seitens der Administration gestartet wurde, konnte sich die öffentliche Aufmerksamkeit in erster Linie auf die Inhalte der E-Mails und weniger auf den Umstand der ausländischen Beeinflussung richten, was Trumps Wahlchancen sicherlich nicht minderte. CrowdStrikes Russland-Attribution hatte zwar zumindest zeitnah das Attributionsvakuum gefüllt, erhöhte jedoch in der Folge auch den Druck auf die Regierung, ebenfalls Russland als verantwortlich zu benennen. Wird der Darstellung CrowdStrikes als defensivem Proxy in diesem Fall ge-

folgt, wurde der Nutzen derer Funktionserfüllung vonseiten der Obama-Administration überschätzt, da im weiteren Verlauf (August 2016) sogar russische Störversuche gegen die US-Wahlinfrastruktur entdeckt wurden und somit das ›Naming-and-Shaming‹ seitens des Privatsektors zur Abschreckung weiterer Maßnahmen offensichtlich nicht ausgereicht hatte.[132]

Eine weitere Frage, die an dieser Stelle gestellt werden muss, ist die nach dem Einfluss der damaligen Umfragewerte auf das Kalkül der Obama-Regierung: Sämtliche Umfragen sahen Clinton über den gesamten Wahlkampfzeitraum hinweg als die wahrscheinliche Siegerin mit teilweise kaum aufzuholendem Vorsprung an (Mercer et al. 2016). Somit bleibt fraglich, ob Obama die Wahrung der eigenen Neutralität auch im Falle eines vorhergesagten Wahlsieges Trumps so lange vor einem entschlossenen Vorgehen gegen die russischen Beeinflussungsmaßnahmen präferiert hätte.

Bevor nun mit Donald Trumps Präsidentschaft fortgefahren wird, werden zwei weitere Vorfälle herausgegriffen: Anhand des Sony-Hacks kann die Bedeutung der wahrgenommenen Verwundbarkeitsasymmetrien der USA gegenüber dem jeweiligen Cyberkontrahenten verdeutlicht werden. Als das Unternehmen am 24. November 2014 durch nordkoreanische Hacker angegriffen wurde, veröffentlichte das FBI bereits einen Monat später ein Attributions-Statement, das das Regime in Pjöngjang verantwortlich machte. Am selben Tag bezog sich Präsident Obama zudem in einer öffentlichen Rede auf den Vorfall und kündigte eine US-Reaktion an, die er jedoch nicht weiter spezifizierte. Als es am 27. Dezember 2014 in Nordkorea zu einem weitflächigen Internet-Shutdown kam, attribuierte Pjöngjang die USA als Verantwortlichen (CBS News 2014). Auch wenn sich die USA hierzu nicht direkt bekannten, befeuerten Aussagen eines republikanischen Abgeordneten diese Theorie noch weiter (Fisher 2015). Der Internet-Shutdown lässt sich durch das anders geartete Verwundbarkeitsverhältnis zwischen den USA und Nordkorea zum damaligen Zeitpunkt als zwischen den USA und Russland 2016 beschreiben. Zum einen war das nordkoreanische Intranet durch dessen zentralisierten Charakter weitaus anfälliger für solch einen Shutdown, andererseits verfügt Pjöngjang abseits seines Nuklearwaffen-Programms über weniger Eskalationspotenziale gegenüber Washington als der Kreml. Hinzu kommt, dass sich die USA in weitaus reduzierterem Maße in Interdependenzverhältnissen mit Nordkorea befinden als etwa mit China auf wirtschaftlicher und mit Russland auf sicherheitspolitischer Ebene.

Im Falle des Sony-Hacks können jedoch auch die Interessen all jener als mitentscheidend für die entschlossene, politische Handlung angesehen werden, die den ›American Way of Life‹ bislang erfolgreich in alle Welt exportiert und somit den amerikanischen Softpower-Status hergestellt hatten. Dass ein Angriff auf die Redefreiheit in US-Unterhaltungsprodukten als direkte Aggression gegen die ideellen Werte und Interessen der USA auf Grundlage des ersten Verfassungszusatzes gewertet wurde, spiegelte sich daher auch in folgender Aussage Obamas wider: »*We cannot have a society in which some dictator someplace can start imposing censorship here in the United States*« (Obama, zitiert in: Holland &

132 Die von Obama auf seiner letzten Pressekonferenz im Jahr 2016 berichtete Warnung an Putin, er solle mit der Wahlstörung aufhören, die er an ihn im September 2016 gerichtet habe, kann somit als Einsicht dieser bislang defizitären Reaktionen auf Russlands Vorgehen gewertet werden (vgl. Jacobs 2016).

Spetalnick 2014). Wie bereits beschrieben, stand Obama vielen AkteurInnen aus ›Hollywood‹ zudem besonders nahe, weshalb ihm auch besonders daran lag, deren Interessen zu schützen.

Der zweite Fall von Interesse ist die Sabotage-Kampagne der russischen APT Sandworm gegen ukrainische Stromversorger 2015 und 2016. Gerade weil die USA nicht direkt betroffen waren, ist deren Attributionsverhalten hierbei besonders aufschlussreich: Bei den Operationen handelte es sich nach Stuxnet um die aufsehenerregendsten Beispiele physischer Sabotage durch Cyberangriffe, zudem gegen kritische Infrastrukturen und somit illegitime Ziele physischer Konfliktmaßnahmen entsprechend des ›ius in bello‹. Trotz dieses Umstandes konnten sich die USA erst im Jahr 2020 und infolge bereits getätigter Attributionen, Sanktionen und Anklagen gegen russische Militärangehörige zu einer öffentlichen Attribution und Reaktion in Form einer Anklageerhebung durchringen. Direkt nach den Sabotageakten hatte es allenfalls durchgestochene Attributionsstatements einzelner PolitikerInnen gegeben (Perez 2016). Hätten die Operationen US-Ziele betroffen, wäre eine ähnliche Zurückhaltung nur schwer vorstellbar gewesen. Zu diesem Zeitpunkt wollten die USA Russland aufgrund des Ukraine-Krieges sowie der Frontstellung im Syrien-Krieg mutmaßlich zu keiner weiteren gegen US-Ziele gerichteten Konflikteskalation provozieren. Hinzu kommt, dass die eigenen Stromnetzwerke ähnlich schwach gegen solche Cyberangriffe geschützt waren (Sternstein 2016). Daher könnten die Attributionen der US-IT-Unternehmen in diesem Falle ebenfalls als Proxy-Attribution gewertet werden, wird davon ausgegangen, dass die USA trotz allem ein Interesse daran hatten, Russland öffentlich als Verantwortlichen zu benennen.

5.6.3.4 Donald Trump, der Handelskonflikt mit China und eine noch offensivere Cyber-Strategie

> »China is neither an ally or a friend — they want to beat us and own our country.«
> *Donald Trump auf seinem Twitter-Account »@realDonaldTrump« am 21. September 2011*
>
> »It could be Russia, but it could also be China. It could also be lots of other people […] It also could be somebody sitting on their bed that weighs 400 pounds.«
> *Donald Trump über den DNC-Hack 2016, zitiert in Starks (2016)*

Nicht nur für den Stil sowie die Inhalte der US-Politik im Allgemeinen, sondern auch für deren Strategie im Cyberspace brachte die Amtsübernahme durch Donald Trump zu Beginn des Jahres 2017 Änderungen mit sich. Bevor entsprechend der beiden Amtszeiten Barack Obamas auch die ideellen sowie wirtschaftlichen Interessen der Trump-Administration analysiert werden, sollen zunächst diverse Veränderungen auf der republikanischen, d.h. institutionellen Ebene auf der Cyberebene diskutiert werden.

Unter Trump kam es zur Absetzung des unter Obama implementierten Cyber Security Coordinators, um den Abstimmungsbedarf zwischen den einzelnen Behörden zu verringern und deren Arbeit effizienter zu gestalten. In diesem Zusammenhang kann ebenfalls die Modifizierung der ›Presidential Policy Directive 20‹ unter Trump genannt werden, die dem US CYCOM größere Autonomie bei der Durchführung offensiver Cyberoperationen einräumte und somit politische Zustimmungsbefugnisse reduzierte (Borghard und Lonergan 2018). Zweitens gibt es seit mehreren Jahren Debatten über den Zeitpunkt der anzustrebenden Trennung zwischen NSA und CYCOM auf der Leitungsebene,

da beiden Behörden aktuell dieselbe Person vorsteht. Vorangetrieben wurden die Diskussionen während der Amtszeit von Trump u.a. durch das Erreichen der ›Full Operational Capability‹ der Cyber Mission Force im Jahr 2018 sowie nicht zuletzt durch das Versagen beider Behörden im Zuge des SolarWinds-Hacks. Dabei wurde konkret in Frage gestellt, inwiefern aufgrund der zunehmenden Komplexität von nachrichtendienstlich unterstützten Cyberoperationen diese Aufgabe noch einer Person überantwortet werden sollte (Borghard 2021).

Nichtsdestotrotz kam auch zwischen 2017 und 2021 der auf internationaler Ebene vertretene Multistakeholder-Ansatz des US-Cyberökosystems zum Ausdruck, an dem verschiedene AkteurInnen der staatlichen, militärischen, zivilen sowie privatwirtschaftlichen Ebene beteiligt sind (auch ›Whole-of-Nation‹ oder ›Whole-of-Systems‹-Ansatz). Diese pluralistische Interessensvertretung wird hauptsächlich durch den National Security Council gebündelt bzw. koordiniert (IISS 2021a, S. 16–17). Inwiefern sich die Trump-Administration entgegen ihrer sonstigen Präferenz für bilaterale ›Deals‹ und Abkommen speziell im Bereich der internationalen Cyberattributionen stärker auf gemeinsame Erklärungen stützte, wird im weiteren Verlauf von besonderem Interesse sein.

Nachfolgend werden drei Leitinteressen Trumps und dessen BeraterInnenkreises behandelt. Hierdurch sollen die auffälligsten Besonderheiten dessen offensiver Cyberstrategie sowie der veränderten Attributionspolitik erklärt werden.

Der Handelskonflikt mit China: »*Make America Great Again*«

Quasi als außenpolitisches Pendant zu seinem innenpolitischen Feindbild der Demokratischen Partei entwickelte sich recht schnell für Präsident Trump die Regierung in Peking heraus. Wie das oben genannte Twitter-Zitat verdeutlicht, vertrat Trump seine konfliktive Haltung gegenüber China schon viele Jahre vor Beginn seiner politischen Karriere. Auch im Wahlkampf hatte er immer wieder darüber gesprochen, wie er als Präsident mit China umgehen würde: »*We can't continue to allow China to rape our country and that's what they're doing. It's the greatest theft in the history of the world*« (Donald Trump, zitiert in: Stracqualursi 2017). Genau wie der ›Sumpf‹ der liberal-kapitalistischen Eliten an der Wallstreet und in Washington das Volk der Amerikaner jahrelang ›beraubt‹ hätte, habe auch China die Errungenschaften der USA im Industrie- und Technologiesektor gestohlen.

Bereits 2017 entwickelte sich daher zwischen den USA und China der oftmals auch als ›Handelskrieg‹ bezeichnete Konflikt zwischen Washington und Beijing, in dem im Rahmen eines ›Tit-for-Tat‹ die Verhängung von Strafzöllen und Wirtschaftssanktionen erfolgte (Dollar und Petri 2018). In dieser Frontstellung kam die Präferenz Trumps und seiner engsten, aus dem rechts-populistischen Spektrum stammenden Berater wie Steve Bannon nach einer zunehmend konfliktiven Außenpolitik gegenüber China zum Ausdruck. Die Bestrebungen Pekings nach der Verwirklichung des ›chinesischen Traums‹ sowie die zunehmende Beteiligung und teilweise auch Kontrolle digitaler Infrastrukturprojekte nicht nur in Entwicklungsländern, sondern auch im Rahmen von 5-G-Projekten in Europa, stellten aus Sicht Trumps eine direkte Bedrohung seines Vorsatzes dar, Amerika wieder ›great‹ zu machen (Kharpal 2018). Indem zu Beginn lediglich chinesische, später aber auch europäische Unternehmen mit Strafzöllen etwa auf Stahl und Aluminium belegt wurden, wollte Trump eines seiner Wahlversprechen wahrmachen: Die US-BürgerInnen der mittlerweile oftmals abgehängten traditionellen

Industriezweige des Rust Belts sollten wieder zu GewinnerInnen gemacht werden. Die Jahre der Obama-Regierung stellte Trump dagegen als eine Art Ausverkauf amerikanischer Interessen dar, sowohl auf wirtschaftlicher als auch sicherheitspolitischer Ebene.

Wie bereits dargestellt wurde, stieg bereits für Obama der Druck, entschiedener gegen chinesische Cyberspionage vorzugehen. Die Interessensverfolgung Pekings war immer konfliktiver gegenüber den wirtschaftlichen Interessen vieler US-Unternehmen geworden, da deren asymmetrische Verwundbarkeit seitens China immer stärker ausgenutzt worden war. Im Gegensatz zu Obama bewertete Trump nun aber den Nutzen einer eskalativ-konfrontativen Strategie gegenüber China höher als deren Kosten: So schadeten die im Laufe der vier Jahre verhängten Strafzölle Chinas als Vergeltungsmaßnahme für protektionistische Handlungen der USA Studien zufolge der US-Wirtschaft im erheblichen Maße (Polaski und Dollar 2020). Darüber hinaus spielten in Trumps Präferenzordnung die bestehenden Interdependenzen mit alliierten demokratischen Staaten offensichtlich nur eine untergeordnete Rolle. So nahm er in Kauf, dass die Durchsetzung seines eigenen Interesses nach stärkerem US-Protektionismus eben nicht nur US-Unternehmen, sondern in der Folge besonders europäische Unternehmen betraf, die er ebenfalls mit Strafzöllen, z.B. gegen die dominante Autoindustrie, belegte (Goulard 2020, S. 60). An dieser Stelle wird deutlich, dass Trump die bislang bestehende US-EU-Interessenskonvergenz auf ideeller Ebene als weniger bedeutsam einschätzte als das Durchsetzen der eigenen Wirtschaftsinteressen. Somit spielte er entsprechend seiner illiberal-populistischen Prägung unterschiedliche Interessensgruppen gegeneinander aus bzw. stellte deren Interessensdurchsetzung zunehmend als Nullsummenspiel dar, in dem die USA nur auf Kosten anderer, auch befreundeter Staaten gewinnen könnten.

Wie der HD-CY.CON zeigt, attribuierten US-IT-Unternehmen während der Präsidentschaft Trumps regelmäßig und in großer Häufigkeit chinesische Cyberoperationen mit staatlicher Beteiligung. Von den erfassten 30 Attributionen fallen 12 in das Jahr 2018, in dem der Handelskonflikt durch das erstmalige Erlassen von Strafzöllen seitens der USA begonnen und stetig intensiviert wurde (Reuters 2020c). Bemerkenswert ist jedoch, dass nur in zwei von 12 Fällen zusätzlich zur technischen Attribution auch eine politische erfolgte. Eine Erklärung hierfür könnte sein, dass die technischen Attributionen nichts mit der übergeordneten Anti-China-Strategie der USA zu tun hatten. Da sich die USA bereits in einem Handelskonflikt mit China befanden, sahen sie auch weniger Notwendigkeit für eigene Attributionen chinesischer Spionageakte, um potenzielle Gegenreaktionen zu legitimieren.

Dass in lediglich drei von 18 Fällen, in denen eine US-Anklage gegen chinesische Hacker als Attributionsquelle verzeichnet wurde, auch eine US-IT-Attribution kodiert wurde, die zudem zweimal erst nachgelagert erfolgte, stützt die These einer fehlenden Staat-Proxy-Beziehung unter Trump.[133] Wie das oben angeführte Zitat von Trump verdeutlicht, maß dieser Attributionen privatwirtschaftlicher AkteurInnen, aber auch seiner eigenen Geheimdienste lediglich in Abhängigkeit von deren Nutzen für seine eigenen Zie-

133 Es handelt sich hierbei nicht um 18 verschiedene Anklageschriften, da sich manche davon auf mehrere Fälle im Datensatz beziehen.

le eine Bedeutung bei. Die bereits erwähnte Attribution-by-Indictment-Strategie sollte somit wohl eher nicht als direktes Resultat einer Anweisung Trumps gewertet werden.[134] Vielmehr resultierte sie vermutlich aus zwei unterschiedlichen Entwicklungen: Erstens der zunehmenden Aggressivität einer steigenden Anzahl autokratischer Staaten im Cyberspace, allen voran China, Russland, Iran und Nordkorea, sowie zweitens der nach wie vor defizitären Reaktionsstrategien demokratischer Staaten hierauf. So signalisieren öffentliche Anklagen zwar Kenntnis über die Machenschaften des Gegenübers, legen Taktiken offen und schränken bestimmte HackerInnen in ihren Bewegungsmöglichkeiten ein. Bislang konnten sie Autokratien jedoch in der Folge nicht effektiv daran hindern, weitere Cyberoperationen gegen demokratische Ziele durchzuführen. In Ermangelung einer effizienten Bearbeitung von Cyberkonflikten auf internationaler Ebene und im Rahmen des Völkerrechts stellten Anklageerhebungen somit unter Trump vermutlich die Fortsetzung dieses bereits durch Obama begonnenen Weges dar. Gegenüber China konnten sie jedoch kaum noch zu Konzessionen führen, da Trump den Konflikt auf der konventionellen Ebene zuvor bereits eskaliert hatte.

Das erwähnte Unternehmen Recorded Future, das wie FireEye durch In-Q-Tel gesponsert wurde, könnte als möglicher Cyberproxy während der Trump-Präsidentschaft plausibilisiert werden. So erscheint aufgrund dieser Beziehung zur CIA zumindest eine Abstimmung über inhaltliche Fokussierungen der Insikt Group und deren Attributionen plausibel, was deren zahlreiche Attributionen chinesischer APTs ab 2017 reflektieren. Hierbei könnte jedoch der Fokus neben einem wohl auch intendierten ›Naming-and-Shaming‹ der chinesischen Hacker zusätzlich auf der Stärkung der Resilienz der anvisierten Ziele gelegen haben.

Während Trumps Präsidentschaft starteten die USA nicht nur einen veritablen Handelskonflikt mit China, sondern forcierten auch eine Intensivierung ihrer eigenen Cyberangriffsbemühungen. Im Rahmen der bereits zuvor länger seitens des DoD propagierten Strategien ›Defending Forward‹ (zuvor ›Hunt Forward‹) und ›Persistent Engagement‹ gaben die USA ihre zumindest verbale Zurückhaltung gegenüber der eigenen Cyberoffensive auf. Künftig solle ein regelmäßiger Konfliktaustrag mit China, Russland, Iran und Nordkorea verstärkt stattfinden, diese Staaten sollten direkt in ihren Systemen attackiert und die Angriffslinie solle somit dorthin verschoben werden. Die öffentlich bekannt gewordenen Cyberoperationen der USA zwischen 2017 und 2021 legen nahe, dass dieser Ansatz weniger China umfasste, da keine spezifischen Offensivoperationen gegen chinesische Ziele bekannt wurden.[135] Anders verhält es sich jedoch vor allem auch gegenüber dem Iran: Wie sich das US-Offensiv- sowie -Attributionsverhalten gegenüber dem Regime in Teheran unter Trump veränderte, wird Gegenstand des nachfolgenden Abschnitts sein. In den beiden Offensivdoktrinen kam zudem die bereits angesprochene Präferenz der Trump-Administration für uni-, bzw. bilaterale Politiken zum Ausdruck,

134 Experteninterview mit Brandon Valeriano, Mitglied der US-Cyber-Solarium-Commission, am 28.09.2020.

135 Anonyme US-Beamte zählten 2020 in einem Medienbericht jedoch auch China zu den von CIA-Cyberoperationen betroffenen Ländern Ray 2020. Im Gegensatz zur Operation gegen die IRA in St. Petersburg vor den Zwischenwahlen 2018, sowie den noch vorgestellten Operationen gegen iranische Ziele 2019 & 2020, wurden hierüber jedoch keine weiteren Details bekannt.

da deren praktische Anwendung de facto das Hacken der Netzwerke auch alliierter Staaten notwendig machte (Smeets 2020). Aus diesem Grund wird zuletzt Trumps Verhältnis zu den NATO-Staaten diskutiert und untersucht, welchen Einfluss dies auf die US-Cyberpolitik hatte.

»*Maximum Pressure*«: Die Aufkündigung des Joint Comprehensive Plan of Action (JCPOA)

Neben dem Versprechen, Amerika auf ökonomischer Ebene zu altem Glanz zu verhelfen, umfassten Donald Trumps Wahlversprechen auch ein aggressiveres Vorgehen gegen den Iran. Nachdem seine Aussagen vor der Wahl 2016 jedoch widersprüchlich waren, ob er den Deal aufkündigen oder lediglich nachverhandeln wolle (Torbati 2016), entschied er sich 2018 für die erste Option. Zuvor hatten innerhalb der US-Administration der damalige nationale Sicherheitsberater Herbert Raymond McMaster sowie Außenminister Rex Tillerson Berichten zufolge Trump immer wieder vor einem solchen Schritt abgehalten (Landler 2018). Dies änderte sich, als sie 2018 ihrer Ämter enthoben und durch John Bolton sowie Mike Pompeo ersetzt wurden. Diese drängten Trump zu einem aggressiveren Vorgehen gegen den Iran und letztlich der Aufkündigung des JCPOA. Jedoch nicht nur Mitglieder der US-Administration nahmen Einfluss auf Trumps Entscheidung: So berichtete die New York Times, dass ein enger Berater der Vereinigten Arabischen Emirate sowie Saudi-Arabiens seinen persönlichen Zugang zu Donald Trump stetig intensiviert hatte und diesen wie Bolton und Pompeo zum Rückzug aus dem Nukleardeal drängte (Kirkpatrick und Mazzetti 2018). Auf republikanischer Ebene hatte sich der Modus Operandi der domestischen Interessensvertretung unter Trump stetig ›privatisiert‹, indem persönliche Kontakte zum Präsidenten zur Umgehung formal-demokratischer Entscheidungsprozesse und Kontrollmechanismen führten (Hill 2021). Politik wurde nicht mehr primär im Rahmen demokratischer Institutions- und Konsultationsformen ausgehandelt, sondern vor allem im Rahmen informeller Treffen auf Trumps Anwesen in Florida.

Die Aufkündigung des JCPOA im Rahmen der ausgerufenen Iran-Politik des ›Maximum Pressure‹ nahm Einfluss auf das US-Cyberoffensivverhalten gegenüber dem Iran, jedoch auch umgekehrt. Mit dem JCPOA verband die Obama-Administration auch die Hoffnung, dass hierdurch die seit Stuxnet gestiegenen iranischen Cyberoperationen gegen US-Ziele eingehegt werden könnten. Diese gingen zwar nicht gänzlich zurück, fokussierten sich nach der Unterzeichnung des Abkommens öffentlichen Quellen zufolge jedoch stärker auf subtilere Operationsformen, etwa Cyberspionage. Zuvor hatten DDoS-Angriffe gegen US-Banken im Rahmen der ›Operation Ababil‹ 2012, die Hacks gegen den New Yorker Damm 2013 sowie das Sands Casino 2014 erhebliches Aufsehen in den USA erregt (Perlroth 2021, S. 278).

Auch im HD-CY.CON wurden für die Startjahre 2015, 2016 und 2017 keine disruptiven Cyberoperationen gegen US-Ziele staatlichen AkteurInnen oder Cyberproxys des Irans angelastet, jedoch sieben Cyberspionageoperationen, was einen Teilerfolg dieses intendierten ›Issue-Linkage‹ der Obama-Administration andeutet. Auch nach 2017, dem Jahr der Amtsübernahme Donald Trumps, änderte sich im Datensatz dieses Muster nicht, es wurden sechs ausschließliche Cyberspionageoperationen iranischer Proxys/staatlicher AkteurInnen auf (u.a.) US-Ziele erfasst. Dies könnte einerseits als

Evidenz gewertet werden, dass der Iran vor einer erneuten Intensivierung disruptiverer Operationsformen gegen US-Ziele trotz der Trump-Aggressionen zurückschreckte. Andererseits hatten sich seit 2012/2013 die iranischen Cyberfähigkeiten erheblich ausgeweitet, deren Angriffe wurden immer sophistizierter. DDoS-Operationen können zwar kurzfristig zu Chaos beim anvisierten Ziel führen und auch eine Signalwirkung entfalten, versprechen jedoch generell keine langfristigen Mehrwerte aus sicherheitspolitischer Sicht. Cyberspionage gegen US-Behörden, WissenschaftlerInnen, Think Tanks oder Unternehmen stellte dagegen für den Iran eine willkommene Möglichkeit dar, sowohl auf sicherheitspolitischer als auch wirtschaftlicher Ebene bestehende Asymmetrien zu seinem Vorteil auszunutzen bzw. die eigenen Verwundbarkeiten, etwa infolge von Wirtschaftssanktionen der USA, zu reduzieren (vgl. Zettl 2022).

Nichtsdestotrotz markiert besonders das Jahr 2019 einen Wechsel der US-Cyberpolitik gegenüber dem Iran: Infolge zunehmender Konflikte auf der konventionellen Ebene im Nahen Osten setzte die Trump-Administration verstärkt auf Cyberoperationen als Reaktion. Als der Iran im Juni 2019 eine US-Drohne über der Straße von Hormus abschoss, antworteten die USA mit einer disruptiven Cyberoperation des CYCOM gegen eine Datenbank der iranischen Revolutionsgarden, mit deren Hilfe sie ihre Angriffe auf Öltanker koordiniert hatten. Zuvor hatte Trump im Rahmen der ›Defending-Forward‹-Doktrin die Befugnisse der CIA zur Durchführung offensiver Cyberoperationen gestärkt (Hanna 2019). Drei Monate später beschuldigten die USA gemeinsam mit Alliierten den Iran, für einen Raketenangriff auf Anlagen des saudischen Ölunternehmens Saudi-Aramco verantwortlich gewesen zu sein. Auch hier reagierten die USA laut Medienberichten mit Cyberoperationen, die die Propagandafähigkeiten Teherans anvisierten. Zuvor war bereits bekannt geworden, dass iranische Cyberangreifer (›Phosphorous‹) versucht hatten, gezielt die E-Mail-Accounts von Personen aus dem Umfeld Trumps im Rahmen seiner (Wieder-)wahlkampagne zu infiltrieren (Ali und Stewart 2019). Als sich im Wahljahr 2020 die iranischen Revolutionsgarden in E-Mails an US-WählerInnen als Akteure der rechten Gruppierung ›Proud Boys‹ ausgaben, diesen darin drohten und das US-Wahlsystem diskreditierten, antworteten die USA ebenfalls durch Cyberoperationen (Cohen 2020). Deren Art und Zielrichtung wurden jedoch nicht weiter spezifiziert, verantwortlich zeichnete sich jedoch wieder CYCOM.

Wie zuvor 2018, hackten die USA somit Ziele autokratischer Cyberangreifer, die versucht hatten, die US-Wahlen zu stören, wenn nicht gar zu beeinflussen. Zum Ausdruck kommen hier ferner die hinreichende Koordination der Geheimdienste untereinander sowie deren erhöhte Zusammenarbeit mit den Betreibern sozialer Medien, weiteren Unternehmen, WissenschaftlerInnen sowie ausländischen PartnerInnen im Vorfeld der Wahlen 2020 (Nakashima 2020). Besagte Akteure verfolgten somit im Rahmen eines ›Whole-of-Nation‹-Ansatzes das Interesse, die US-Wahlen zum einen maximal zu schützen, andererseits jedoch im Gegensatz zu 2016 die BürgerInnen auch zeitnah und transparent über die erlassenen Maßnahmen zu informieren. So attribuierte der damalige Direktor der Geheimdienste, John Ratcliffe, bereits 27 Stunden nach Bekanntwerden der Fake-E-Mails die IRGC als verantwortliche Partei. Keine öffentliche US-Attribution zuvor wurde schneller durchgeführt (Nakashima 2020). Diese Interessen gerieten infolge des Wahlsiegs Joe Bidens jedoch zunehmend in Konflikt mit Donald Trumps Ansinnen einer Diskreditierung der Wahl als »*rigged*«, was ihn etwa dazu veranlasste,

den damaligen CISA-Chef Chris Krebs zu feuern. Dieser hatte zuvor die Wahl als eine der sichersten überhaupt bezeichnet (Geller 2020).

Zwei Aspekte stechen aus der Cyberkonfliktinteraktion zwischen den USA und dem Iran unter Trump heraus: Erstens unterstreicht die Wahl offensiver Cyberoperationen als Reaktion auf konventionelle Militärschläge des Iran das Ansinnen der USA, den Konflikt mit dem Iran in der Region nicht vollständig zu einer kriegerischen Auseinandersetzung werden zu lassen. Auch wenn dies Trump zeitweise erwog, entschied er sich letztlich doch dagegen, auch aufgrund mutmaßlich zu hoher Kollateralschäden. Eigene, offensive Cyberoperationen werden somit von demokratischen Regierungschefs bislang wohl eher als deeskalierendes Konfliktmittel angesehen, wie auch schon im Abschnitt zur US-Entscheidung für Stuxnet deutlich wurde.[136] Zweitens legt die Form der Selbstattribution der USA durch geleakte Informationen an US-Medien, die lediglich anonyme Regierungsquellen zitierten, eine gewisse Unsicherheit der Administration bezüglich der rechtlichen Legitimation ihrer Operationen nahe. Wären sich die USA sicher gewesen, dass ihre Operationen internationalem Recht vollumfänglich entsprachen, hätten sie durch eine offizielle Bekanntgabe und Kommentierung ihrer Operationen ein noch deutlicheres Signal, auch an Freunde und Verbündete senden können. Rote Linien wären noch eindeutiger kommuniziert und die Anwendung internationalen Rechts im Cyberspace wäre gestärkt worden. Dass dies jedoch nicht der Fall war, indiziert, dass die USA befürchteten, durch ein öffentliches Eingeständnis ihrer Operationen einen gefährlichen Präzedenzfall nicht nur für verfeindete, sondern auch für befreundete Staaten zu schaffen. Beides konnte für die USA als generell risikoaverses Land nicht im eigenen Interesse liegen (vgl. Kaminska 2021).

Die unter Trump durchgestochenen Selbstattributionen belegen zudem den veränderten Verschleierungsfokus im Gegensatz zur Überwachungspraxis der NSA: nicht mehr die Geheimhaltung der Operation an sich war das Ziel. Auch wenn in beiden Fällen (*Geheimhaltung der Operation an sich* vs. *Verschleierung der eigenen Verantwortlichkeit*) verfassungsrechtliche Rechenschaftspflichten vermieden werden soll(t)en, können nur bei der Selbstattribution auch die Vorteile einer »offenen Geheimhaltung« ausgenutzt werden (vgl. Cormac und Aldrich 2018, S. 479.[137] Dies betrifft etwa das *Signaling* eigener Absichten und Fähigkeiten, was künftig besonders für demokratische Staaten interessant sein könnte, die gerade im Begriff sind eigene Cyber Commands aufzubauen.

Dass die eigenen Offensivoperationen unter Trump jedoch nicht nur das Verhältnis zu autokratischen Kontrahenten, sondern auch zu demokratischen Alliierten beeinflussten, ist Gegenstand des folgenden Abschnitts.

---

136 Bereits im Dezember 2021 hatten jedoch Politiker und IT-Experten aus den USA argumentiert, dass russische Cyberoperationen gegen ukrainische Ziele im Rahmen des sich zuspitzenden Konflikts als Indikator für eine bevorstehende Militärinvasion des Landes gewertet werden könnten, was dafürspricht, dass für eigene und fremde Cyberoperationen unterschiedliche Eskalationsbewertungen vorgenommen, bzw. unterschiedliche Eskalationskalküle auf der Seite autokratischer AngreiferInnen angenommen werden (Miller 2021).

137 Dies ist somit eine Parallele zur autokratischen Verwendung offensiver Proxys, z.B. im Rahmen disruptiver, sichtbarer Operationen.

Die USA als ›ausgenutzte‹ Weltmacht: Trump und die NATO

Das Verhältnis zwischen Donald Trump und der NATO war bereits seit Beginn seiner Präsidentschaft belastet. Trump machte keinen Hehl daraus, dass er das Bündnis als Verlustgeschäft für die USA als größten Nettozahler betrachtete. Zudem kommen zahlreiche Staaten der Vereinbarung, mindestens zwei Prozent des nationalen BIPs in das Verteidigungsbudget zu investieren, seit Jahren nicht nach (Bergmann und Cicarelli 2021). Trumps Skepsis gegenüber IOs und deren multilateralen Entscheidungsprozessen beschränkte sich jedoch nicht nur auf die NATO. Bereits zu Beginn seiner Amtszeit kündigte er die Teilnahme der USA am Handelsabkommen der ›Trans-Pacific Partnership‹ auf und schloss in der Folge zahlreiche bilaterale Abkommen mit Ländern wie Japan oder Südkorea (Erb und Sommers 2020). Im August 2019 stießen die USA europäische Alliierte mit ihrer Entscheidung vor den Kopf, den INF-Vertrag mit Russland aufgrund der Nichteinhaltung der Vertragsbestandteile durch Russland auszusetzen (Bugos 2019). Die USA demonstrierten an dieser Stelle somit eine eingeschränkte Sensibilität gegenüber europäischen Sicherheitsinteressen. Zuletzt kündigten die USA unter Trump im Juni 2020 an, ein Jahr später aus der WHO austreten zu wollen. Die Entscheidung wurde zwar seitens der Biden-Regierung wieder zurückgenommen, verdeutlicht jedoch die stärkere Gewichtung nationaler Interessen aus Sicht des Präsidenten Trump gegenüber gemeinschaftlichen Interessen der Staatengemeinschaft. So warf Trump der WHO inmitten der Corona-Pandemie vor, Desinformationen über das Virus für das Regime in Peking zu verbreiten (Nichols 2020).

Insgesamt war der US-Alleingang gegenüber China im Rahmen des Handelskrieges sicherlich am prägnantesten. Jedoch auch das Aufkündigen des JCPOA 2018, gegen den Willen der ebenfalls involvierten alliierten Vertragspartner, vertiefte die Konfliktivität der Präferenzkonstellationen des transatlantischen Bündnisses. Der Bruch in den Beziehungen ging so weit, dass Trump engen Beratern zufolge wiederholt seine Absicht geäußert hatte, aus der NATO austreten zu wollen. Akteure der Administration, etwa der ehemalige Chief of Staff John F. Kelly, konnten ihn jedoch hiervon abbringen (Crowley 2020).

Neben dieser Präferenz Trumps für bilaterale Deals und gegen IOs wie die NATO stachen in seiner Amtszeit jedoch gemeinsame Attributionserklärungen mit alliierten oder befreundeten Staaten heraus. Im Februar 2018 stimmten die übrigen Five-Eyes-Mitglieder mit dem öffentlichen Statement Großbritanniens überein, dass Russland für die NotPetya-Kampagne 2017 verantwortlich sei (Muncaster 2018).[138] Zwei Monate später folgte ein gemeinsamer technischer Bericht des britischen NCSC, des FBI und DHS, der stärker die Resilienz-Funktion auf technischer Ebene erfüllen sollte (NCSC 2018a). Diese Praxis entspricht der engen geheimdienstlichen Kooperation der Länder innerhalb des Bündnisses, die zunehmend schadhafte Cyberoperationen autokratischer Staaten inkludiert.

138 Bereits im Dezember 2017 hatten die USA und Großbritannien parallel Nordkorea für die WannaCry-Kampagne verantwortlich gemacht und auf die Übereinstimmung dieses Befundes mit den Erkenntnissen der anderen Five Eyes-Mitglieder verwiesen Corera 2017. Dabei handelte es sich jedoch um kein gemeinsam verfasstes schriftliches Statement.

Im Oktober 2018 kam es zu einer ebenfalls vermutlich koordinierten Attributionskampagne. Dabei lasteten die Niederlande und Großbritannien in einer gemeinsamen Erklärung dem russischen GRU den versuchten OPCW-Hack sowie die Vergiftung des ehemaligen russischen Geheimdienstagenten Sergei Skripal in Salisbury an (Gov.UK 2018). Am selben Tag veröffentlichte zudem das US DoJ eine Anklage gegen GRU-Mitglieder wegen des Hacks der WADA, der IAAF sowie des Unternehmens Westinghouse Electric (DoJ 2018d). Ebenfalls am 4. Oktober veröffentlichte ferner Kanada ein Statement, in dem Russland für den WADA-Hack verantwortlich gemacht wurde (Government of Canada 2018).

Im Februar 2020 kam es zu koordinierten Attributionsstatements Georgiens, Großbritanniens, der EU und weiterer Staaten, in denen die GRU-Einheit 74455 für die umfassenden DDoS- und Defacement-Operationen gegen georgische Ziele am 28. Oktober 2019 verantwortlich gemacht wurde. Tatsächliche Evidenzen für diesen Befund enthielten die Veröffentlichungen jedoch nicht. Dass somit nun auch die EU und weitere europäische Staaten gemeinsam mit den Five-Eyes-Ländern eine koordinierte Attribution tätigten, kann wohl auch in zeitlichem Zusammenhang mit der Weiterentwicklung der Cyber Diplomacy Toolbox der EU gesehen werden. Die erstmalige Anwendung von Sanktionen als Bestandteil der Toolbox befand sich zu diesem Zeitpunkt wohl bereits in Vorbereitung und erfolgte im Juli 2020. Auch in diesem Zusammenhang wurde die Bedeutung zwischenstaatlichen, in diesem Falle transatlantischen Informationsaustauschs zwischen den Geheimdiensten deutlich, da sich die EU auch auf Evidenzen und Erkenntnisse der US-Behörden stützte (Bendiek und Schulze 2021, S. 25). Andererseits konnten die USA Cozy Bear als Eindringling in die Netzwerke des DNC 2016 nur anvisieren, da sie zuvor der niederländische Geheimdienst AIVD auf deren Hackingoperation aufmerksam gemacht hatte.

Innerhalb der US-Administration zeichnete für diesen verstärkten ›Attributions-Multilateralismus‹ laut Experten-Meinungen besonders die erste Cybersicherheitsdirektorin der NSA und heutige ›Deputy National Security Advisor for Cyber and Emerging Technology‹, Anne Neuberger, verantwortlich.[139] Die unter der Leitung von Neuberger veranlasste Informierung Microsofts über einen bestehenden Zero-Day-Exploit durch die NSA stellte Anfang 2020 eine bemerkenswerte, wenn vielleicht auch lediglich punktuelle Abkehr des Geheimdienstes in seiner Praxis des Sammelns und Geheimhaltens von Software-Sicherheitslücken dar (O'Neill 2020b). Der Fall verdeutlicht jedoch, wie das berichtete Interesse Neubergers an einem verbesserten Informationsaustausch zwischen dem öffentlichen und Privatsektor auch Einfluss auf das Verhalten der NSA insgesamt nahm. Daher ist davon auszugehen, dass dies auch zu einer schwächeren Oppositionshaltung der NSA gegenüber gemeinsamen staatlichen Cyberattributionen führte.[140] Voraussetzung hierfür kann jedoch nur gewesen sein, dass besagte Verant-

139 Experteninterview mit Dr. Brandon Valeriano, Mitglied der US-Cyber-Solarium-Commission, am 28.09.2020.

140 Auch auf nationaler Ebene kam es zu ›Joint Attributions‹ verschiedener US-Behörden, etwa im Falle der gemeinsamen Erklärung von CISA, DoJ, ODNI und NSA am 5. Januar 2021, dass Russland für die SolarWinds-Kampagne verantwortlich sei (CISA 2021). Dieses Vorgehen entspricht aus liberaler Perspektive dem ›Whole-of-Government‹-Ansatz.

wortlichkeitszuweisungen nicht zu viele Detektions- und Attributionsmethoden der Geheimdienste offenlegten.

Die am 19. Juli 2021 seitens des DoJ veröffentlichte Anklage gegen drei chinesische MSS-Angehörige sowie einen Mitarbeiter eines Frontunternehmens, der im Auftrag des MSS über sieben Jahre lang Regierungen, Unternehmen und Universitäten weltweit hackte, deutet einen unter Joe Biden triadischen Attributionsweg der USA an. So wurde am Tag der Anklageveröffentlichung ein gemeinsames Attributionsstatement der USA, ›Allies and Partners‹ veröffentlicht, das »*Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China*« *u.a.* auch den Microsoft-Exchange-Hack, attribuiert (The White House 2021). Zudem veröffentlichten CISA, NSA und FBI ein ›Joint Cybersecurity Advisory‹ mit einem Schwerpunkt auf der Beschreibung des technischen Vorgehens der chinesischen Hacker. Individuelle Anklagen als nationale Strategie der Attribution, gepaart mit international abgestimmten ›Joint Statements‹ sowie national koordinierten technischen Berichten, könnten zur prävalenten US-Strategie im Falle von Cyberoperationen werden, vorausgesetzt jedoch, dass sich mit entsprechenden ›Allies and Partners‹ auch ein entsprechender Attributionskonsens finden lässt. Dieser Ansatz entspricht aus liberaler Theorieperspektive stärker dem ›Whole-of-System-Approach‹, der eine behörden-, länder- und systemübergreifende Kooperation im Cyberspace vorsieht und sich gleichzeitig an unterschiedliche Adressaten richtet.

Einerseits zeichneten sich die USA unter Trump somit durch einen Hang zum Rückzug aus multilateralen Foren und Verträgen sowie nationale Alleingänge aus. Andererseits etablierte sich seit 2017 die Praxis der ›Joint Attributions‹ in unterschiedlicher Form und mit meistens unterschiedlichen TeilnehmerInnen. Aus liberaler Sicht kann argumentiert werden, dass Trump zwar Einfluss auf die offensive Ausrichtung der nationalen Cyberstrategie der USA nehmen konnte, da es hierfür besonders im DoD bereits zuvor BefürworterInnen gegeben hatte. Gleichzeitig konnte er seine Präferenz zur Relativierung geheimdienstlicher Evidenzen (vor allem gegen Russland), die seinen eigenen Interessen widersprachen, im Bereich der Attribution nicht entscheidend durchsetzen. Die US-Geheimdienste schafften es somit, ihren Informationsaustausch intern, mit dem Privatsektor und ausländischen Geheimdiensten zumindest auszuweiten. Informationsasymmetrien wurden (in Teilen) aufgegeben und bewusste Abhängigkeiten aufgebaut, um die gemeinschaftliche Verwundbarkeit gegenüber autokratischen CyberangreiferInnen zu reduzieren. Laut ExpertInnen konnten hierfür die ›Defending-Forward‹- und ›Persistent-Engagement‹-Strategien sogar als hilfreich angesehen werden, da diese für Attributionen wichtige Informationen über das technisch-operative Vorgehen der Kontrahenten lieferten.[141]

Die wichtige Rolle der Geheimdienste demokratischer Regierungen im Rahmen von Attributionsprozessen kann auch die zumindest verbale Zurückhaltung europäischer Staaten gegenüber der Offensivdoktrin der Trump-Regierung erklären. Ähnlich wie zuvor infolge der Snowden-Enthüllungen konnten auch vermehrte Cyberoperationen der USA in den eigenen Netzwerken besagte Länder wohl nicht davon überzeugen, den bedeutenden Informationsaustausch im Rahmen von Cyberoperationen zu riskieren.

141 Experteninterview mit Dr. Erica Borghard, Mitglied der US-Cyberspace Solarium Commission, am Interview am 06.10.2020.

Hinzu kommt, dass eben jene Länder zumindest in der Theorie sogar von dieser Praxis profitieren könnten, falls die US-Operationen tatsächlich zu Informationsgewinnen über das Vorgehen der autokratischen Kontrahenten führen und sie diese auch mit den als ›Sprungbrettern‹ fungierenden Ländern teilen.

5.7 Demokratisches Fallbeispiel II: Israel

»Israel is blessed with many opponents, and as such, it developed core competencies mostly in the defense sector in order to be able to protect itself.«
Dudu Mimran, CTO des Cyber Security Research Center der Ben-Gurion Universität, zitiert in: Moersen (2018).

Israel zeichnet sich nicht nur durch seine Lage in einer durch gewaltsame Konflikte geprägten Region aus, sondern auch durch ein hohes Maß an Digitalisierung. Gerade im militär-industriellen Komplex weist das Land ein hohes Maß an Innovation auf. Militärische Überlegenheit nicht nur im konventionellen, sondern auch im Cyberraum dient der Sicherung des eigenen Überlebens in einer aus israelischer Sicht weitgehend feindlich geprägten Nachbarschaft (s. das obere Zitat). Die nachfolgende Studie des israelischen Cyberkonfliktverhaltens bzw. der Attributionspraktiken israelischer IT-Unternehmen dient als Abgleich mit den USA als ›Best Case‹: Können nur für die USA als technologischer Vorreiter Evidenzen für eine defensive Cyberproxy-Beziehung gefunden werden? Oder zeigen sich auch für weitere, technologisch fortgeschrittene Demokratien wie Israel derartige Tendenzen? Die unter 5.2.3 hierfür bereits ausgemachten Indizien bilden die Basis für die nun folgende Analyse der beiden AVs.

5.7.1 Israelische Cyberattributionen: Wer macht was?

Für den zweiten demokratischen Untersuchungsfall Israel sind in erster Linie die 31 im Datensatz enthaltenen Fälle relevant, in denen israelische IT-Unternehmen als eine der ›Attribution-Bases‹ erfasst wurden. In elf der 31 Fälle waren israelische Ziele unter den Opfern. Bemerkenswert ist jedoch, dass in keinem der elf Fälle eine politische Attribution erfasst wurde.

In 28 der 31 Fälle stellten israelische IT-Unternehmen nicht nur die Attributionsquelle dar, sondern machten den Vorfall auch als Erste öffentlich. Diese beiden Befunde sprechen für die Funktion des Resilienzaufbaus durch die Detektionen und Attributionen, jedoch nicht nur für israelische Ziele entsprechend des internationalen Kundenportfolios der israelischen IT-Unternehmen.

Die Anzahl der Vorfälle, in denen israelische IT-Unternehmen eine staatliche Verantwortlichkeit bei den AngreiferInnen attribuierten (n = 24), folgt im Zeitverlauf entsprechend des Jahres der Attribution keinem offensichtlichen Muster (Abbildung 35). Auch wenn deren Anzahl ab 2014 insgesamt steigt, fällt sie im Jahr 2018 zwischenzeitlich ab.

Der längerfristige Trend bis 2019 impliziert jedoch wie für die gesamte Branche einen Anstieg israelischer IT-Attributionen, insbesondere, da die Zahlen für die Jahre 2020 und 2021 vorläufig sind. Jedoch müssen diese Beobachtungen insofern relativiert werden, als sich die Attributionshäufigkeiten in den jeweiligen Jahren im Vergleich zu den USA auf relativ niedrigem Niveau bewegen.

Die 31 Fälle technischer Attributionen gilt es nun hinsichtlich der attribuierten *Initiator-Categorys* zu analysieren.

Staatlich gesponserte Proxys wurden somit am häufigsten seitens der israelischen IT-Unternehmen attribuiert, gefolgt von nichtstaatlichen AkteurInnen (Initiator-Categorys 3,1 – 3,5). In drei Fällen wurde keine Akteurskategorie attribuiert, jedoch zumindest ein vermutetes Ursprungsland der Operation angegeben. Lediglich in zwei Fällen detektierten IT-Unternehmen aus Israel zudem einen Vorfall, gaben jedoch weder Initiator-Category noch -Country an. ›True Attributions‹, also Verantwortungszuweisungen, die den Akteur und dessen Herkunftsland benennen, machen für israelische IT-Unternehmen 25 Fälle und somit 80,6 Prozent der 31 Attributionen aus.

Dass die israelischen IT-Unternehmen besonders häufig eine Proxy-Attribution vornehmen, kann auch hier auf die prävalente Nutzung von Cyberproxys durch Autokratien hindeuten, andererseits jedoch auch auf eine mögliche Zurückhaltung der IT-Unternehmen, noch häufiger Staaten direkt verantwortlich zu machen.

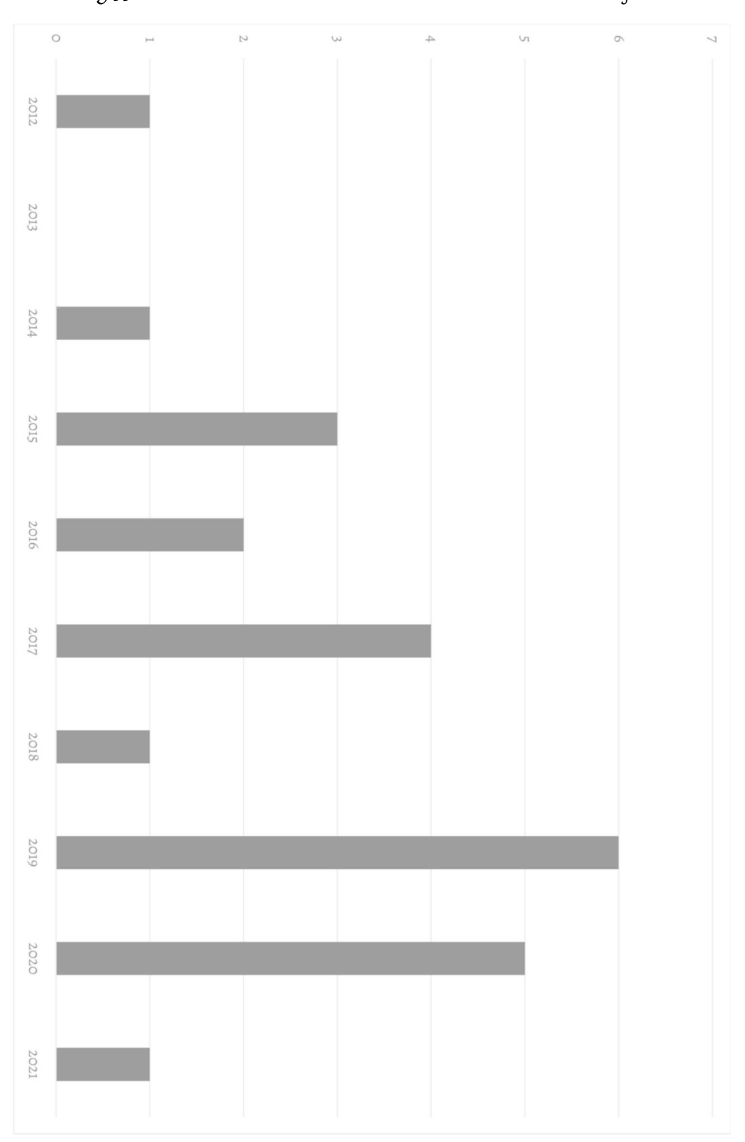
Die elf Cyberoperationen mit u.a. israelischen Zielen, die von israelischen IT-Unternehmen attribuiert wurden, richteten sich in absteigender Häufigkeit besonders gegen folgende Sektoren: politische/staatliche AkteurInnen/Institutionen, kritische Infrastrukturen (insbesondere den Verteidigungssektor), Unternehmen und Forschung/Bildung, Medien/JournalistInnen und ZivilakteurInnen. Damit decken sie alle Sektoren ab, die regelmäßig von staatlichen AkteurInnen angegriffen werden. Abbildung 37 zeigt die Verteilung der attribuierten Initiator-Countrys.

Die gelisteten Länder entsprechen dem ambivalenten Profil israelischer IT-Unternehmen: Einerseits sind sie fest verankert durch ihre israelische Herkunft, wodurch sich der Fokus auf den Iran und Palästina erklären lässt, andererseits sind sie oftmals international anerkannt und im Cyberspace aktiv, was den Fokus auf chinesische Cyberoperationen plausibel macht.

Wie bereits erwähnt, wurde in keinem der 31 Fälle mit israelischer IT-Attribution gleichzeitig eine Verantwortungszuweisung politischer AkteurInnen aus Israel im HD-CY.CON verzeichnet. Dies könnte als Indiz für die Erklärungskraft der Proxy-Funktion der Reduzierung politischen Handlungsdrucks/Signaling gewertet werden. Dies heißt nicht, dass sich israelische Regierungsbeamte überhaupt nicht zu Cyberoperationen in der Öffentlichkeit äußerten. Jedoch taten sie dies zumeist in generischer Weise, im Sinne einer Art ›Catch-All-Attribution‹ gegenüber Kontrahenten wie dem Iran. So warf der damalige Premierminister Benjamin Netanjahu dem Iran, Palästina und dem Libanon 2013 vor, »*nonstop*« Cyberoperationen gegen israelische Ziele auszuführen, ohne dabei jedoch konkretere Details zu nennen (Reuters 2013). Hinzu kommt, dass israelische PolitikerInnen und BeamtInnen in Teilen Angriffe auf die eigenen Netzwerke selbst öffentlich machten, jedoch mit dem Zusatz, dass staatliche Stellen deren Erfolg hätten verhindern können (s. Soffer 2014). Diese Selbstdetektion von vereitelten

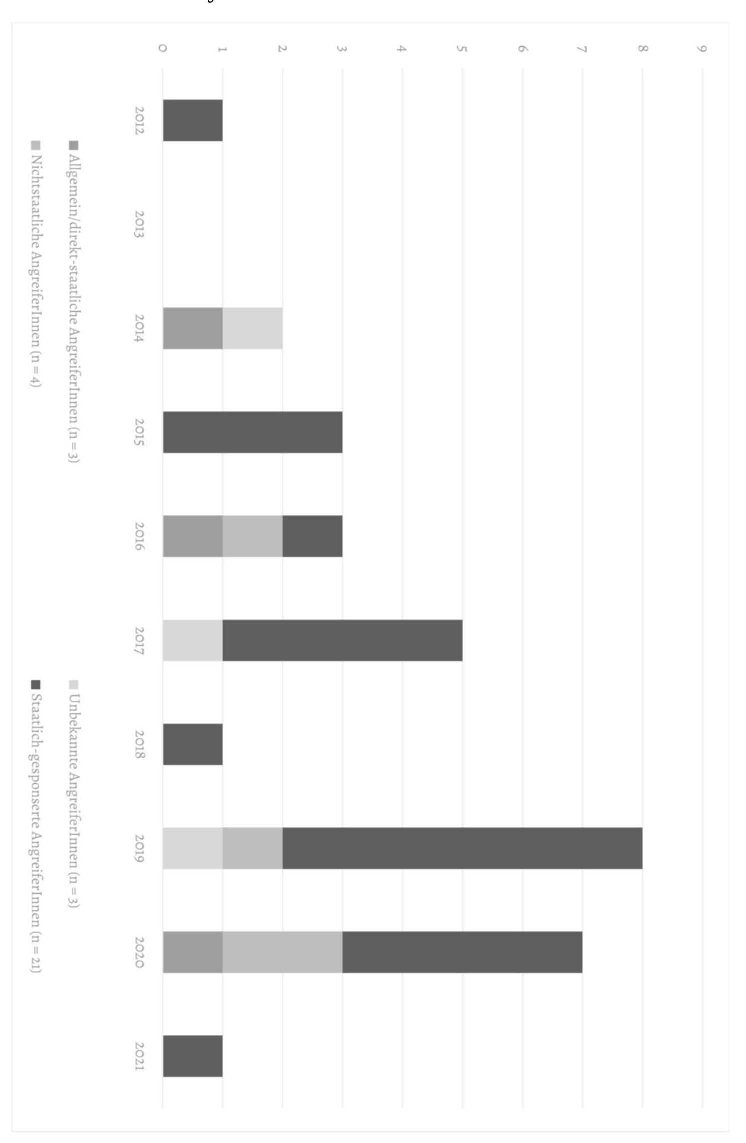
Cyberoperationen dient offensichtlich der Legitimations- und Reputationsstärkung der eigenen Defensivfähigkeiten.

Abbildung 35: Attributionen israelischer IT-Unternehmen im Verlauf der Zeit



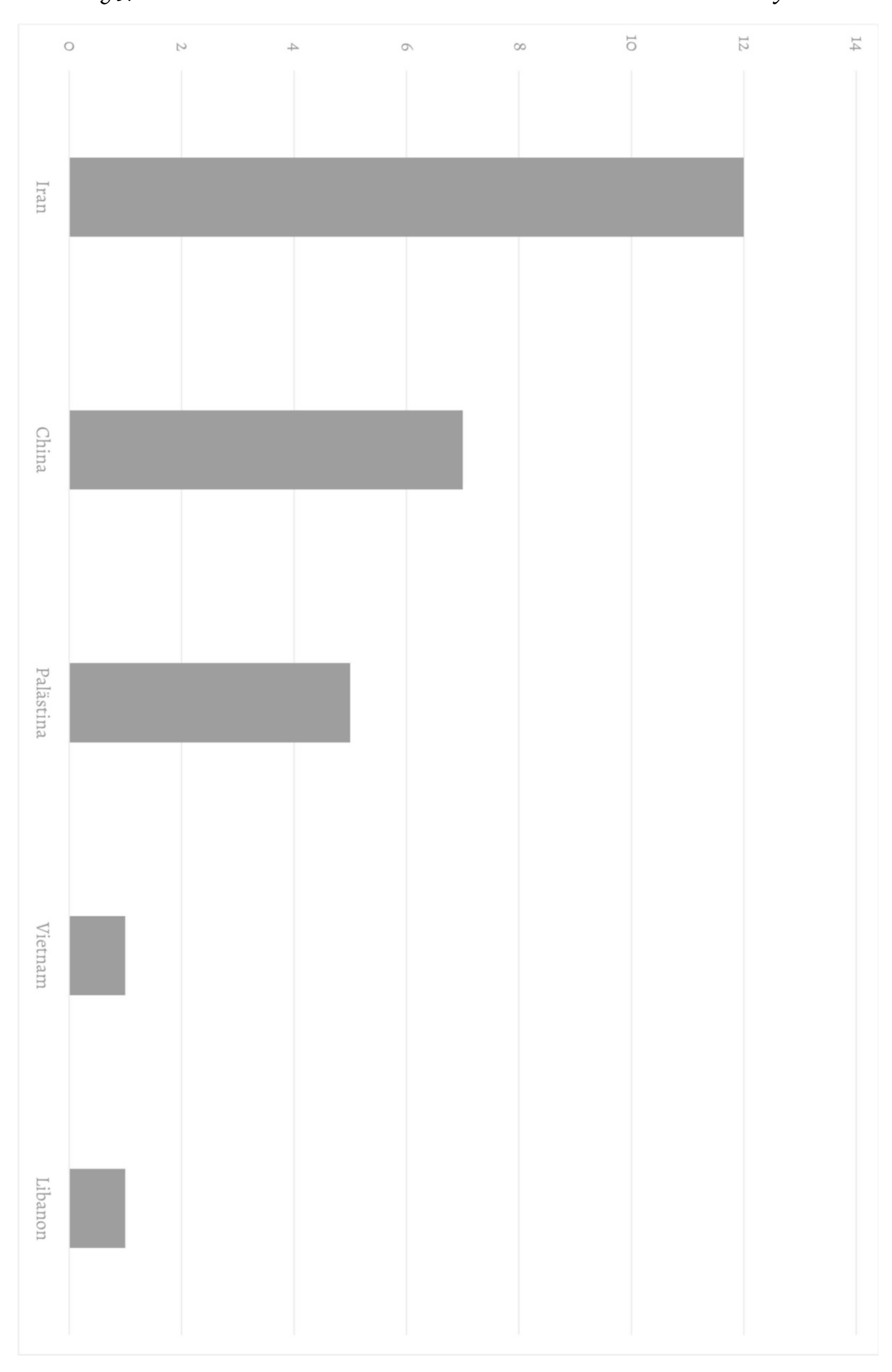
(Eigene Darstellung auf Basis des HD-CY.CON)

Abbildung 36: Die attribuierten Initiator-Categorys der israelischen IT-Unternehmen im Zeitverlauf



(Eigene Darstellung auf Basis des HD-CY.CON)
Hinweis: Die Zahlen beziehen sich ausschließlich auf die Attributionen der israelischen IT-Unternehmen in den jeweiligen Fällen, auch wenn diese nicht die einzigen Attributionsquellen waren. Das Attributionsjahr wurde für die Fälle, in denen israelische IT-Unternehmen keine staatliche Involvierung auf der Angreiferseite attribuierten, zum Zwecke der Arbeit nachkodiert und sind nicht im HD-CY.CON enthalten.

Abbildung 37: Die seitens israelischer IT-Unternehmen attribuierten Initiator-Countrys



(Eigene Darstellung auf Basis des HD-CY.CON)

Im Jahr 2020 kam es zu einer durchgestochenen Attribution israelischer Beamter. Bei dem Vorfall handelte es sich um einen Cyberangriff mutmaßlich iranischer Hacker gegen die zivile Wasserinfrastruktur Israels (Staff 2020). Da der Fall jedoch auch 2020 stattfand, ist er kein Bestandteil des HD-CY.CON. Dennoch ist er aus mehreren Gründen interessant: Erstens verdeutlicht er das anscheinend bestehende Interesse Israels an politischer Attribution, vor allem gegenüber dem Iran. Dass dies jedoch nicht in offizieller Form getan wurde, könnte auf fehlende Attributionsevidenzen oder den Unwillen der Regierung hindeuten, diese offen zu legen. In der Folge wurden anonyme US-Beamte in der Washington Post zudem mit der Aussage zitiert, Israel habe als Antwort auf die iranische Cyberoperation die Systeme eines iranischen Hafens gehackt (Warrick und Nakashima 2020). Dass nichtgenannte US-Beamte einen Vergeltungsschlag Israels an die Medien durchstechen, könnte als Attributions-Koordination zwischen den USA und Israel gewertet werden.

Auf Basis dieser Befunde kann die Cyberproxy-Funktion der ›Schaffung von Legitimation politischer Attributionen‹ für Israel nicht als erklärungskräftig bewertet werden. Stattdessen sprechen die präsentierten Zahlen stärker für die Proxy-Funktionen der ›Reduzierung politischen Handlungsdrucks/Signaling‹ sowie einer Steigerung der technischen sowie soziopolitischen Resilienz, jedoch nicht nur israelischer ZielakteurInnen.

Tabelle 21 listet die im Datensatz verzeichneten israelischen IT-Unternehmen auf:

Tabelle 21: Israelische IT-Unternehmen als Attributionsquellen im HD-CY.CON

Rang	Unternehmen	Vorkommen im HD-CY.CON
1	Check Point	12 (Threat-Reports); 2 (Medienzitate)
2	ClearSky	6 (Threat-Reports); 3 (Medienzitate)
3	Cyberreason*	6 (Threat-Reports)
4	AVNET*	1 (Medienzitat)
5	Seculert	1 (Medienzitat)
6	SentinelOne*	1 (Threat-Report)
7	CyberX*	1 (Threat-Report)

(Eigene Darstellung auf Basis des HD-CY.CON)
Anmerkung: Die Gesamtzahl ergibt hier 33 und nicht 31, da auch die beiden Fälle inkludiert sind, in denen israelische IT-Unternehmen den Fall lediglich öffentlich machten.
*Der Hauptsitz dieser Unternehmen ist zwar (teilweise durch Übernahmen seitens US-Konzernen) mittlerweile in den USA, ihre Gründer sind jedoch Israelis und identifizieren sich und ihr Unternehmen auch noch mit ihrem Herkunftsland (vgl. Magistretti 2017; Div 2018; Williams 2020; IT Times 2020).

An erster Stelle rangiert das Unternehmen Check Point. In zehn der 14 Fälle, in denen eine Attribution von Check Point erfasst wurde, implizierten diese eine staatliche Involvierung auf der AngreiferInnenseite. Fünfmal vermutete das Unternehmen jeweils den Iran sowie China als verantwortliches Land, einmal den Libanon und Nordkorea. Auch

diese Verteilung verdeutlicht die dualistische Prägung israelischer IT-Unternehmen mit sowohl domestischer als auch internationaler Ausrichtung. Auf dem zweiten Platz rangiert das Unternehmen ClearSky mit neun erfassten Verantwortungszuweisungen. Hier sahen drei Fälle eine staatliche Mitverantwortung vor, zwei Vorfälle wurden nichtstaatlichen AngreiferInnen aus Palästina angelastet. In fünf Fällen attribuierte Clearsky den Iran.

Wie aus Tabelle 21 zudem hervorgeht, wurde in der Mehrzahl der Fälle durch einen umfangreichen Threat-Report attribuiert, was ebenfalls als Indikator für die Proxy-Funktion der ›Schaffung technischer Resilienz‹ gewertet wird.

Im Gegensatz zu den USA wird aufgrund des Fehlens von Fällen mit gleichzeitiger technischer und politischer Attribution israelischer AkteurInnen nun das Profil der verzeichneten IT-Unternehmen genauer untersucht. Somit soll plausibilisiert werden, inwiefern die vermutete Proxy-Funktion der ›Reduzierung politischen Handlungsdrucks/Signaling‹ tatsächlich als erklärungskräftig für sie angesehen werden kann.

Check Point

Als ›israelisches FireEye‹ kann das Unternehmen Check Point gelten. 1993 von Gil Shwed, dem heutigen CEO, gegründet, entwickelte es im Lauf der Zeit umfassende Kapazitäten im Bereich der Threat-Intelligence. Laut eigener Webseite betreut Check Point mittlerweile einen Kundenstamm von mehr als 100 000 Organisationen mit den eigenen Cybersicherheitsprodukten (Check Point 2021a). Sowohl die Geschäftsleitung als auch der Vorstand weisen einen überwiegend israelischen, jedoch auch amerikanischen Hintergrund auf (Check Point 2021b). Die Biografie des Gründers Gil Shwed steht gewissermaßen stellvertretend für viele seiner Start-up-CEO-Kollegen: Im Alter von 18 Jahren trat er seinen in Israel verpflichtenden Militärdienst in der Unit 8200 an, der zentralen Cyberoperations-Einheit der Israeli Defense Forces (IDF). Diese ist besonders auf elektronische Kriegsführung und Code-Entschlüsselung spezialisiert. Laut Aussage eines Mitglieds der Einheit sehen deren Aufgaben die Integration von »*offensive cyber tools as well as tools that help shape perception, alongside cyber defense*« vor, ein ähnliches Profil wie bei NSA und GCHQ (Zitun 2016, zitiert in: Cordey 2019, S. 8). Nach Beendigung des Militärdienstes gründete er 1993 zusammen mit Shlomo Kramer und Marius Nacht Check Point (Kannunikova 2021). Wie Shlomo Kramer arbeitete auch die heutige Chief Product Officer des Unternehmens, Dorit Dor, in der Unit 8200, wo sie und Shwed sich kennen lernten.

Das Beispiel von Check Point verdeutlicht bereits den großen Stellenwert der Fluktuation zwischen dem Militärsektor und der Privatwirtschaft im israelischen IT-Bereich: Die Unit 8200 dient(e) dabei zahlreichen heutigen CEOs erfolgreicher IT-Unternehmen als ›Sprungbrett‹. Hier erlernten sie ihre technischen Fähigkeiten und bauten sich ihr persönliches Netzwerk auf, von dem sie als angehende EntrepreneurInnen profitieren konnten (Ungerleider 2013). Die Aussicht auf eine erfolgreiche Karriere als Unternehmer äußerten diverse Alumni der Unit 8200 als bedeutenden Anreiz für ihr Engagement in der Einheit (Behar 2016).

Aufgrund der engen Verquickungen zwischen Check Point-Gründern und MitarbeiterInnen mit der Unit 8200 erscheint eine Proxy-Rollenübernahme durch das Unternehmen im Bereich der Attribution plausibel. Dass dies jedoch nicht für alle Fälle

angenommen wird, verdeutlicht das zweigeteilte Attributionsprofil Check Points mit Schwerpunkten auf iranischen und chinesischen CyberangreiferInnen. Nichtsdestotrotz erscheint es wahrscheinlich, dass der oftmals beschriebene Technologie- und Wissenstransfer zwischen Militär und Privatsektor nicht ohne Gegenleistung erfolgt und auch Attributionen zumindest vorher koordiniert werden könnten.

Auffällig ist bei Check Point zudem, dass das Unternehmen in manchen Fällen auch zu niedrigschwelligen Cyberoperationen Attributionsaussagen tätigt, wie etwa für eine Defacement-Operation im Jahr 2020,[142] deren Ursprung das Unternehmen in der Türkei, dem Gaza-Streifen und Nordafrika vermutete (Bachner 2020). Da die Defacement-Nachricht eine direkte Drohung gegenüber Israel beinhaltete (»*The countdown of Israel destruction has begun since a long time ago* [sic!]«; zitiert in: Bachner 2020) und zudem ein Video mit bombardierten israelischen Städten zeigte, lässt sich die im Vergleich zu anderen Defacement-Operationen, etwa von Anonymous, gesteigerte Aufmerksamkeit israelischer IT-Unternehmen erklären.

ClearSky

Das am zweithäufigsten im HD-CY.CON verzeichnete IT-Unternehmen aus Israel, ClearSky, wurde 2012 von Boaz Dolev gegründet. Dolev war zuvor Leiter des israelischen E-Government-Programmes (ClearSky 2021) sowie an der Gründung des ersten Cybersecurity Operation Centre Israels beteiligt (Solomon 2017). Öffentliche Quellen gaben in der Vergangenheit zudem darüber Auskunft, dass auch bei ClearSky diverse MitarbeiterInnen ehemalige Angehörige der Unit 8200 sind (Solomon 2017). Analog zu Check Point deutet somit auch bei ClearSky vieles darauf hin, dass Attributionen zumindest in einzelnen Fällen als Proxy-Tätigkeit angesehen werden können.

In einem Fall aus 2020, der demnach kein Bestandteil des Datensatzes ist, attribuierte das israelische Verteidigungsministerium einen von staatlichen Stellen vereitelten Cyberspionagevorfall der APT Lazarus gegen israelische Verteidigungsministerien, ohne dabei jedoch Nordkorea als dahinter stehenden staatlichen Sponsor zu benennen (Ministry of Defense Israel 2020). Dass das IT-Unternehmen ClearSky genau einen Tag danach in einem umfangreichen technischen Bericht zu der Operation Nordkorea direkt benannte (»Operation Dream Job«; ClearSky 2020), erscheint zum einen als eine Art ergänzende und zeitlich abgestimmte Attribution zur politischen Verlautbarung und liefert zum anderen ausführliche Details zur Stärkung der Resilienz anvisierter AkteurInnen in Israel.

142 Daher ist diese Operation nicht im HD-CY.CON enthalten (2000 – 2019).

Neben den vier weiteren im Datensatz erfassten Unternehmen (AVNET, Cyberreason,[143] Seculert,[144] CyberX[145]) könnte zudem Palo Alto Networks als israelisch kodiert werden, da dessen Gründer Nir Zuk aus Israel stammt und ebenfalls Mitglied der Unit 8200 war (Dor 2021). Vor der Gründung des Unternehmens arbeitete Zuk zudem für Check Point. Wie unter 5.6.1 bereits dargestellt, wurde es jedoch aus folgenden Gründen im HD-CY.CON als amerikanisch eingestuft:

1. Palo Alto Networks Hauptsitz befindet sich (zum Zeitpunkt der Kodierungen) in den USA, im Gegensatz etwa zu Check Point, das diesen nach wie vor in Tel Aviv hat;
2. Palo Alto Networks Geschäftsführung weist einen deutlich transnationaleren Charakter auf als z.B. Check Point (Palo Alto Networks 2021).

Die berichteten Verschränkungen zwischen Militär- und Zivilsektor auf personeller sowie im Rahmen des Israeli Cyber Company Consortium institutioneller Ebene (Sheva 2020) stechen im internationalen Vergleich deutlich heraus. Das hohe Ausmaß an sektorenübergreifendem Technologie- sowie Personentransfer wird als Grundlage dafür angesehen, warum israelische Akteure als *»pioneers in the field of offensive cyber defense«* bezeichnet werden (Cristiano 2021, S. 1).[146] Die quantitativen Daten des HD-CY.CON legen eine Prävalenz der Proxy-Funktion der ›Reduzierung politischen Handlungsdrucks/Signalings‹ nahe, in Abwesenheit gleichzeitiger politischer Attributionen von israelischer Seite. Auch die Stärkung technischer Resilienz über domestische AdressatInnen hinaus kann für israelische Unternehmen plausibilisiert werden. Durch die Hinzunahme der Unternehmensprofile konnten diese Befunde hinsichtlich einer tatsächlichen Zusammenarbeit zwischen Privatunternehmen und staatlichen Stellen auch bei der Attribution von Cyberoperationen weiter gestärkt werden. Im Rahmen der Analyse der UV wird jedoch diskutiert werden, inwiefern es sich bei Israel um eine besondere Staat-Proxy-Beziehung handelt und ob dies die Anpassung/Spezifizierung der identifizierten Proxy-Funktionen notwendig macht.

---

143 Cybereason wurde trotz seines Hauptsitzes in den USA als israelisches Unternehmen kodiert, da es sich laut eigenen Angaben in erster Linie mit der israelischen Herkunft der Gründer identifiziert (Div 2018). Des Weiteren weist deren Geschäftsführung eine stärker israelische Prägung auf, als etwa Palo Alto Networks. Zudem war CEO und Mitbegründer Lior Div ebenfalls Mitglied der Unit 8200 (Levy 2021). Cybereason machte u.a. damit auf sich aufmerksam, dass sie Operationen der Ransomware-Gruppierung DarkSide bereits vor dem Colonial Pipeline Hack im Mai 2021 in einem Blog Post behandelten (Cybereason Nocturnus 2021).

144 Seculert wurde 2017 vom israelisch-amerikanischen Cybersicherheitsunternehmen Radware aufgekauft. Dessen CEO, Roy Zisapel, war laut eigenen Angaben ebenfalls Mitglied der Unit 8200 (Benjamin 2011).

145 CyberX wurde von zwei Absolventen des ›Israel Defense Force's Center for Encryption and Information Security‹ 2013 gegründet und 2020 von Microsoft aufgekauft (Orbach 2020).

146 Der bei *»offensive cyber defense«* anklingende Widerspruch wird wie für die USA unter Trump auch im Zuge der Analyse der UV für Israel noch diskutiert.

Tabelle 22: Ausprägung der AV I auf Grundlage des HD-CY.CON für Israel

Starke Ausprägung	Schwache Ausprägung
Steigerung der technischen und soziopolitischen Resilienz (Threat-Research-Berichte über chinesische Cyberspionage gegenüber verschiedenen Wirtschaftssektoren; Berichte über iranische Cyberoperationen und deren Social-Engineering-Methoden) Reduzierung des politischen Handlungsdrucks/Signaling bzw. Erweiterung des Handlungsspielraums (IT-Attributionen iranischer Cyberoperationen)	Schaffung von Legitimation politischer Attribution

(Eigene Darstellung)

5.7.2 Israels Cyberakteursumwelt

Israel zeichnet sich sowohl auf staatlicher als auch privatwirtschaftlicher Ebene durch ein hohes Maß an Technologieaffinität aus. Beginnend mit der staatlichen Ebene, weist das Land eine hoch entwickelte Armee auf, besonders in Relation zur geografischen Größe sowie Bevölkerungsanzahl (The Jerusalem Post 2012; Koshkin 2021). Auf die historischen Ursachen hierfür wird im Rahmen der Analyse der UV genauer eingegangen. An dieser Stelle sollen die auf staatlicher Ebene im Laufe der Zeit ausgebildeten Institutionen und Behörden im vor allem militärischen Cyberbereich vorgestellt werden.

Ein zentraler Akteur sind die IDF mit der bekanntesten Unit 8200 (s. Tabelle 23). Diese ist dem Israeli Directorate of Military Intelligence unterstellt (AMAN), das zudem die Unit 9900 (Imagery Intelligence (IMINT)), die Unit 504 (Human Intelligence (HUMINT)) sowie die Unit 81 (Entwicklung offensiver Cybertools) erfasst (Cordey 2019, S. 10). Unit 8200 ist in erster Linie für SIGINT-Aktivitäten, Code-Entschlüsselung und offensive Cyberoperationen zuständig und steht daher zumeist im Fokus der Öffentlichkeit, wenn israelische Cyberoffensivkapazitäten thematisiert werden (s. Tendler 2015; Behar 2016; Stoler 2018; Stern 2019). Unterstützt werden die Mitglieder dieser Einheit direkt durch die Unit 81, die Cyberangriffswerkzeuge entwickelt und bereitstellt (Behar 2016). Unit 8200 umfasste 2019 Berichten zufolge zwischen 5000 und 10 000 Mitglieder, wobei nicht alle davon im aktiven Dienst und vermutlich auch nicht direkt an offensiven Cyberoperationen beteiligt sein dürften (Cordey 2019, S. 16). Nichtsdestotrotz lässt sich diese Anzahl mit dem britischen GCHQ vergleichen, nur dass Großbritannien mehr als sechsmal so viele EinwohnerInnen hat wie Israel.

Den Grundstein für Israels Status als eine der technologisch versiertesten und modernsten Militärmächte haben während des Kalten Krieges aus der Sowjetunion emigrierte Israelis mit entsprechenden Kenntnissen im Bereich der ›Computation-Theory‹ gelegt (Shamir 2005). Als Wendepunkte in der Struktur und Organisationskultur der Unit 8200 werden der Jom-Kippur-Krieg von 1973 sowie der damit verbundene Bericht der ›Agranat Commission‹ gewertet, der sich mit den Defiziten der IDF bei der Antizipa-

tion ägyptischer und syrischer Militärschläge befasste und als dessen Resultat ein neues, grundlegendes Gesetz, ›The Army 1975‹, erlassen wurde, das den rechtlichen Status der IDF festlegte (Peri 1981, S. 311).

In der Folge entwickelte die Unit 8200 ein im Vergleich zu den meisten anderen Geheimdiensten alternatives Rekrutierungssystem, das weniger Wert auf Erfahrung oder den entsprechenden technischen Hintergrund legte, sondern Problemlösungs- und Führungskompetenzen der zudem sehr jungen KandidatInnen in den Vordergrund stellte (Asher-dotan 2018). Dieser Ansatz diente zugleich als Grundlage für die in vielen Fällen im Anschluss an den Militärdienst eingeschlagene Karriere der Unit 8200-Mitglieder als EntrepeneurInnen im Technologiebereich (Valache 2020). Im Rahmen einer eigenen Alumni-Vereinigung fördern ehemalige Mitglieder in ihren neuen Funktionen in der Privatwirtschaft die Vernetzung zwischen Unternehmen und IDF (Solomon 2021).

Aufseiten der Defensive kam es im israelischen Institutionengefüge wie in den meisten anderen Staaten in den letzten zehn Jahren zu einem erheblichen Wachstum. So betonte die 2011 ins Leben gerufene ›National Cyber Initiative‹ die Notwendigkeit einer Umstrukturierung der israelischen Cybersicherheits-Governance, angestrebt durch die Kreierung des ›Israel National Cyber Bureau‹ (INCB) (Adamsky 2017, S. 115–116). Dieses ist direkt dem Premierminister unterstellt. Eine der Hauptaufgaben des INCB war die Verfassung einer nationalen Cybersicherheitsstrategie, die 2017 schließlich verabschiedet wurde (Moersen 2018). Zusammen mit der zwischenzeitlich etablierten ›National Cyber Security Authority‹ (NCSA) wurde das INCB 2018 zentralisiert in das neu gegründete ›National Cyber Directorate‹ überführt (IISS 2021c).

Zuletzt stellen israelische Gerichte als potenzielle Vetospieler der militärischen und zivilen Geheimdienste wie dem Israeli General Security Service (SHABAK; Israels domestische Geheimdienstorganisation) und dem MOSSAD (Israels Auslandsgeheimdienst) einen wichtigen Akteur dar. So hat das Oberste Gericht seit den 1970-er Jahren eine eindeutige Präferenz für eine verstärkte rechtliche sowie gerichtliche Aufsicht der Geheimdienste entwickelt (Bitton 2016, S. 141). Inwiefern sich deren Rolle bei der Aufsicht und Einhegung nachrichtendienstlicher Aktivitäten sowie im Falle der Unit 8200 auch offensiver Operationen im Laufe der Zeit gewandelt hat, könnte somit ebenfalls für die Analyse der UV relevant sein.

Wie beschrieben, entwickelte sich Israel auch im privatwirtschaftlichen Sektor im Technologiebereich zu einem der führenden Länder und wird immer wieder mit dem Titel ›Start-up-Nation‹ bedacht (Yerman 2019; Zerachovitz 2021). Grundlage hierfür war die bereits 1993 und damit sechs Jahre vor dem US-Pendant In-Q-Tel gegründete Regierungsinitiative Yozma. Diese brachte durch steuerliche Anreize ausländische Investoren nach Israel und stockte deren Investitionen in Bereichen wie ›Communication‹, ›Information-Technology‹ und ›Life-Science‹ auf (Yozma 2021). Sogenannte ›Venture-Capital‹-Investitionen in Start-ups nehmen in Israel im Vergleich zu anderen Industrienationen die deutlich wichtigste Bedeutung ein (Stand 2016: 0,3 Prozent des BIP; Röhl 2016, S. 26), wenngleich die USA in absoluten Zahlen nach wie vor die meisten ›Unicorns‹ hervorbringen (Stand 2019; Graham 2019). Unter Berücksichtigung der Bevölkerungszahlen scheint Israel aus relativer Sicht die führende Start-up-Nation zu sein.

Israel bringt jedoch nicht nur regelmäßig erfolgreiche IT-Start-ups im Bereich der Cybersicherheit und Threat-Analysis hervor, sondern auch Unternehmen mit Spio-

nagesoftware als Kernprodukt. Am bekanntesten ist hier die von zwei ehemaligen Unit-8200-Mitgliedern 2010 gegründete NSO-Group (Brewster 2016a). Deren Spionagesoftware Pegasus erregte in den letzten Jahren immer wieder Aufmerksamkeit, da sie bei der Überwachung von MenschenrechtsaktivistInnen, JournalistInnen, Oppositionellen sowie zuletzt im Sommer 2021 auch PolitikerInnen eingesetzt wurde (s. Marczak und Scott-Railton 2016; Scott-Railton et al. 2017; Kenyon 2018; Scott-Railton et al. 2019; Marczak et al. 2020; Kirchgaessner et al. 2021). Laut NSO-Group verkauft sie Pegasus ausschließlich an nationale Regierungen, die Verkäufe müssen durch das israelische Verteidigungsministerium bewilligt werden (O'Neill 2020a).

Im Rahmen des Israeli Cyber Company Consortium kam es ferner auch auf offiziell institutioneller Ebene zu einer Verschränkung zwischen dem öffentlichen und privaten Sektor im Cyberbereich. Dem Konsortium gehören u.a. auch Check Point und Clearsky an (Sheva 2020).

Der Zivilbereich ist in Israel nicht immer eindeutig vom staatlichen und militärischen zu trennen.[147] Fest steht jedoch, dass vor allem im Zuge der allgemeinen Wehrpflicht bereits an Schulen und Universitäten umfangreiche Rekrutierungsbemühungen unternommen werden, um frühzeitig geeignete KandidatInnen für staatliche Cybereinheiten identifizieren zu können. Das Militär und der Privatsektor stehen jedoch in immer stärkerer Konkurrenz zueinander. Da Ersteres mit den Löhnen der Industrie nicht mithalten kann, verfolgt das IDF Berichten zufolge vor allem zwei Strategien: Erstens soll es externe, mutmaßlich durch das Militär finanzierte Unternehmen geben, die höhere Gehälter bei gleichzeitiger Arbeit für den Staat möglich machen,[148] und zweitens wird den OffizierInnen eine längere Militärlaufbahn dadurch schmackhaft gemacht, dass ihnen besonders hohe Gewinne bei einem künftigen Wechsel in die Wirtschaft versprochen werden (Sadeh 2021).

Insgesamt charakterisiert die USA-geprägte Vorstellung einer ›Revolving Door‹ zwischen Regierung und Verteidigungssektor in Israel insbesondere den Cybersicherheits-/-industriekomplex (Boeke und Broeders 2018, S. 82). Letztlich ist wohl in kaum einem (demokratischen) Land die Verschränkung zwischen dem Militär, der Wirtschaft und auch dem Bildungssektor so eng wie in Israel, wovon jedoch alle drei Sektoren profitieren (Reed 2015). Theoretisch gesprochen konditioniert in Israel die Ausprägung der KV somit in erheblichem Maße die prinzipielle Möglichkeit zur Nutzung defensiver, aber auch offensiver Cyberproxys.

Tabelle 23 veranschaulicht die Ausprägungen der einzelnen Teilindikatoren für die Bewertung der KV im Falle Israels.

---

147 »*Once, cyber was a general term. Today, there are subspecialties and expertise of various kinds. There are dozens of such niches within the IDF, and they correspond to niches in the civilian market*«, (Nadav Arbel (CyberHat), zitiert in Sadeh 2021).

148 Insofern es sich bei diesen tatsächlich um durch das Militär finanzierte, offensiv agierende IT-Unternehmen, jedoch ohne vertraglich festgehaltene Rolle als Auftragnehmer handelt, wären diese als offensive Cyberproxys Israels einzustufen.

Tabelle 23: Israels Cyberakteursumwelt auf staatlicher/privatwirtschaftlicher Ebene

NCPI-Teilindikatoren* *(staatliche Ziele)*	Operationalisierung
Cyber Military Doctrine *(Offense)*	IDF Strategy (2015; Cyberspace als ›Fifth Domain‹) National Cybersecurity Strategy (2017; Adamsky 2017)
Cyber Military Staffing/National Cyber Command *(Offense)*	*Militär:* Israeli Directorate of Military Intelligence (AMAN) IDF Unit 8200 (SIGINT, Code-Entschlüsselung, Offensiv-Operationen; Cordey 2019, S. 8) IDF Unit 81 (Entwicklung eigener Technologien, Bereitstellung für andere IDF-Einheiten; Behar 2016) *Zivile Geheimdienste* (Bitton 2016, S. 143): SHABAK (Israels domestische Geheimdienstorganisation) MOSSAD (Israels Auslandsgeheimdienst) *Zusätzliche Akteure der Intelligence Community:* Nachrichtendienstliche Abteilung der Polizei Center for Policy Research Israeli National Cyber Directorate (INCD)
Global Top Technology/Cybersecurity Firms *(Offense, Commercial Gain, Intelligence)*	*U. a.* (Tendler 2015; Morgan 2019): Check Point Clear Sky Cybereason Wix CyberArk Imperva Radware NSO-Group
High-Tech-Exports *(Offense, Commercial Gain, Intelligence)*	Relativer Anteil der High-Tech-Exporte an Gesamtexporten des Landes im Jahr 2008 bei ca. 17 Prozent. Danach stieg der Anteil (im Gegensatz zu den USA) bis 2020 auf ca. 28 Prozent konstant weiter (World Bank 2022a). Der Prozentanteil der R-&-D-Ausgaben am Gesamt-BIP lag bei Israel im Jahr 1998 bei ca. 2,9 Prozent und stieg ebenfalls bis 2020 auf 4,9 Prozent an (World Bank 2022b).

(Eigene Darstellung)

5.7.3 Israels domestische Präferenzkonstellationen und der Einfluss des allgemeinen Konfliktniveaus

Die bisherigen Ausführungen zeigen, dass sich Israel durch einen umfassenden militärisch-industriellen Komplex auszeichnet, der sich in den letzten Jahrzehnten insbesondere der Cyberebene zugewandt hat. Die Verschränkung zwischen den beiden Sektoren scheint noch stärker ausgeprägt zu sein als in den USA, was die ideale Grundlage für die im Rahmen dieser Arbeit konzeptualisierte Proxy-Nutzung bildet (›Revolving Door‹). Im Gegensatz zu den USA konnte die Analyse der beiden AVs jedoch keine Evidenzen für das Wirken der Proxy-Funktion der ›Schaffung von Legitimation politischer Attributionen‹

erbringen. Wie sich diese besonders im Vergleich zu den USA unter Trump noch stärkere Attributionszurückhaltung Israels im Zusammenspiel mit den Verantwortungszuweisungen des Privatsektors erklären lässt, wird Grundlage der Analyse der UV sowie der IV sein. Daher werden in einem ersten Schritt die zentralen Akteursgruppierungen als dominante Teile der Winning Coalition identifiziert, deren Präferenzen darauffolgend zur Erklärung der Ausprägungen der AV untersucht werden.

5.7.3.1 Das Who's Who der israelischen Winning Coalition

Das politische System Israels zeichnet sich durch gleich mehrere zentrale Besonderheiten aus, das es von den meisten anderen, gemeinhin als liberalen Demokratien bezeichneten Ländern unterscheidet: Erstens sieht sich Israel als Nationalstaat des jüdischen Volkes und konstituiert sich somit primär über diese Religionszugehörigkeit, was seit der Verabschiedung des ›Basic Law: Israel – The Nation State of the Jewish People‹ im Jahr 2018 durch die Knesset auch rechtlich kodifiziert ist (Jabareen und Bishara 2019). Zweitens besitzt Israel im Gegensatz zu den westlichen Demokratien keine Verfassung, sondern sog. ›Grundgesetze‹ sowie die Unabhängigkeitserklärung (Neuberger 2008). Drittens wird Israel gemeinhin als die einzige Demokratie im Nahen Osten angesehen und unterscheidet sich somit nicht nur durch das Judentum als Staatsreligion von den muslimischen Nachbarn (Sørli et al. 2005, S. 146). Viertens zeichnet sich Israel durch eine Dominanz des Militärs aus, was zuweilen zur Bezeichnung des Landes als »*Garrison-State*« führte (Simpson 1970).

Besonders der letzte Punkt der oftmals konstatierten Dominanz militärischer AkteurInnen im politischen System gegenüber dem Zivilsektor wurde als Paradox zum gleichzeitigen Status Israels als Demokratie gewertet (Goldberg 2006, S. 377). Als eine mögliche Erklärung hierfür wurde angeführt, dass Israel lediglich auf formal-republikanischer Ebene liberal-demokratischen Anforderungen entspräche, nicht aber tief verwurzelte, ideelle Charakteristika einer liberalen Demokratie besäße, weshalb gleichzeitig die Militarisierung des Staates ermöglicht worden sei (Goldberg 2006, S. 377). Andere BeobachterInnen waren sich lange Zeit darin einig, dass Israel trotz der Militarisierung als parlamentarische Demokratie zu bezeichnen wäre, da seitens der IDF keine ernsthafte Putsch-Gefahr drohe (Cohen 2006, S. 769–770).

Auf institutioneller Ebene dominieren in Israel ideologisch geprägte Parteien das politische System, die auch grob in ›Tauben‹ und ›Falken‹ eingeteilt werden, entsprechend ihrer Haltung in der Palästinenserfrage sowie ihrer (primären) historischen Verwurzelung in der zionistisch-nationalistischen Bewegung (Falken) oder dem Arbeitermilieu (Tauben) (Roberts 2019). Neben dieser Konfliktlinie konstituierte sich das Mehrparteiensystem Israels durch die Unterscheidungen zwischen »*religious and secular sectors, Sephardi and Ashkenazi Jews, Jews and Arabs, rich and poor*« (Brichta 1998, S. 182). Trotz dieser Heterogenität kam es im Laufe der 1950er bis 1970er Jahre zu einer verstärkten Polarisierung des Parteiensystems, das die Likud-Partei (Falken) sowie die Arbeitspartei (bis 1968 ›Mapai‹; Tauben) dominierten, die 1984 schließlich miteinander koalieren (mussten) (Brichta 1998, S. 182–183).

Infolge einer Regierungskrise 1990 kam es zur Einführung des ›Basic Law: The Government‹ im Jahr 1996. Darin wurde die Macht des Premierministers gegenüber den von ihm benannten MinisterInnen und Regierungsbehörden ausgeweitet. Diese konnte er

nun einrichten, aufteilen oder auch auflösen. Als Ausgleich erhielt die Knesset u.a. stärkere Aufsichtsbefugnisse über die Ausrufung eines nationalen Notstands. Dieses Modell wurde als »*premier-parliamentary*« und somit als Hybrid zwischen einem Präsidential- und Parlamentssystem bezeichnet (Brichta 1998, S. 188–189). Als Resultat ging daraus ein gestärkter Premierminister hervor, der jedoch im Gegensatz zum Präsidialmodell noch stärker von seiner eigenen Partei sowie dem Koalitionspartner abhängig ist.

Aus diesen Ausführungen ergibt sich für die nachfolgende Analyse, dass der jeweilige Premierminister und dessen Partei im Untersuchungszeitraum als die erste zentrale Interessensgruppe bzw. Teil der Winning Coalition betrachtet werden. Deren ideologischen sowie kommerziellen Interessen werden als Erstes im Fokus der Analyse stehen. Der Grund dafür ist der privilegierte Herrschaftszugang des von der Partei gestellten Premierministers, der auch den größten Einfluss auf die Außenpolitik des Landes ausübt.

Da ab 2001 nur mit einer kurzen Unterbrechung zwischen 2006 und 2009 die stärker dem rechten Flügel des Parteienspektrums angehörige Likud-Partei den Premierminister stellte, werden deren Präferenzen unter Benjamin Netanjahus Führung von zentraler Bedeutung für die Erklärung der AVs sein.

Als gesonderter Teil der relevanten Interessensgruppen werden zudem die bereits beschriebenen israelischen Geheimdienste in die Analyse eingeschlossen. Aufgrund der besonderen Gründungshistorie des Staates Israels, der sich sein Staatsterritorium gewaltsam erobern musste, nehmen AkteurInnen des militärischen bzw. Verteidigungssektors traditionell eine bedeutende Rolle auch im politischen System ein. Zudem kam es in zahlreichen Fällen zu späteren Wechseln vormaliger zionistischer UnabhängigkeitskämpferInnen in hohe politische Ämter (Ben-Eliezer 2001, S. 149), etwa im Falle des späteren Premierministers Ariel Sharon, der vor der Staatsgründung der Untergrundbewegung Haganah angehörte (Finkelstein 2005, S. 15). Deutlich wird hier bereits, dass aufgrund des gemeinsamen zionistischen Hintergrunds die Interessen der Likud-Partei und Netanjahus als Premierminister mit denen des Militärs und der Geheimdienste grundlegend übereinstimmen könnten. Aufgrund des politischen Eigeninteresses der Wiederwahl sowie der Notwendigkeit, die Unterstützung des Koalitionspartners zu erhalten, wird dennoch davon ausgegangen, dass sich die Interessen dieser beiden Gruppierungen in Teilen auch widersprechen können. Ob dies der Fall war und welchen Einfluss dies auf die Cyberproxy-Nutzung Israels hatte, wird somit Teil der nachfolgenden Analyse sein.

Als dritte Interessengruppe gilt es die Präferenzen des israelischen Rüstungssektors zu analysieren. Wie aufgezeigt, nehmen Unternehmen aus der Verteidigungsindustrie (z.B. Waffenhersteller), zunehmend aber auch aus dem IT-Sicherheitsbereich, eine exponierte Stellung und einen bedeutenden Zugang zu politischen EntscheidungsträgerInnen in Israel ein. Da die Reaktionen Israels vor allem (auch) auf iranische Cyberangriffe erklärt werden sollen, spielen die Interessen der Industrie eine wichtige Rolle, besonders der mit IT-Sicherheit beauftragten Unternehmen. Auch deren Interessen können sich jedoch aufgrund der Dominanz des militärisch-industriellen Komplexes in Israel mit denen militärischer AkteurInnen überschneiden, da beide Seiten gewissermaßen eine überlebenswichtige Symbiose eingegangen sind. Somit sollen auch zwischen

diesen Gruppierungen (wenn möglich) Präferenzkonflikte aufgedeckt und in Bezug zur Ausprägung der AVs gesetzt werden.

5.7.3.2 Benjamin Netanjahu und die Likud-Partei: Der Iran als Staatsfeind Nr. 1, jüdische Hegemonie und der eigene Machterhalt

Für Benjamin Netanjahu und die Likud-Partei werden nachfolgend zwei zentrale, seitens der Forschung identifizierte Interessen analysiert und deren Einfluss auf die israelische Cyberproxy-Nutzung bzw. das israelische Verhalten im Rahmen von Cyberkonflikten wird untersucht: die Bekämpfung des Irans als ›Staatsfeind Nr. 1‹ sowie das Interesse nach jüdischer Hegemonie in Israel. Als drittes gewissermaßen kontinuierliches Leitinteresse wird das seitens der Forschung und ehemaliger MitstreiterInnen betonte Streben Netanjahus nach dem eigenen Machterhalt immer dann in beiden Fällen diskutiert, sofern er diesem gegenüber ideellen oder kommerziellen Interessen den Vorzug gab (vgl. Hoffman 2019; Bergman 2019, S. 623). Entgegen der theoretischen Konzeptualisierung einer illiberalen Demokratie, in der zunehmend die Eigeninteressen der politischen Führung die Politik bestimmen und weniger die Interessen des Selektorats, wird jedoch für Netanjahu aufgezeigt, wie sich dieser flexibel unterschiedlichen Interessen seiner Wählerschaft anpasste und diese dennoch mit seinem persönlichen Machterhalt in Einklang brachte, teilweise gegen den Willen der Geheimdienste.

Bekämpfung des Irans als ›Staatsfeind Nr. 1‹

Als erstes zentrales Interesse Netanjahus und seiner Likud-Partei wird die Bekämpfung des Irans sowie dessen Nuklearwaffenprogramms analysiert. Nachdem Israel während der Regentschaft des Schahs vor der Revolution 1979 eine pragmatische Beziehung zum Land pflegte, änderte sich dies infolge der Ausrufung der iranischen Republik bzw. des Siegs der schiitischen über die säkulare Strömung der Revolution (Sobhani 1989). Die Anti-Israel-Rhetorik des Ayatollah und seiner AnhängerInnen weckte schließlich die schlimmsten Befürchtungen vor einer erneuten existenzbedrohenden ausländischen Macht, die sich explizit gegen Israel als jüdischen Staat richtete (Precht 1988, S. 122–123.) Auch wenn die weiteren muslimischen, jedoch sunnitischen Länder der unmittelbaren Nachbarschaft ebenfalls in den zuvor erfolgten arabisch-israelischen Kriegen militärisch bekämpft wurden, war es die Erwartung einer iranischen Atombombe, die das Land zu einer noch größeren Gefahr aus Sicht Israels werden ließ. Die Angst vor einer iranischen Atombombe lässt sich nochmals in vier Unteraspekte unterteilen: »*fear of annihilation, fear of a more difficult security environment, socioeconomic fears, and fear of a challenge to Israel's founding ideological principles*« (Eiran und Malin 2013, S. 78). Das Interesse Israels an einer Bekämpfung des Irans und seines Atomwaffenprogramms ist somit überwiegend ideell-historisch verwurzelt,[149] betrifft sicherheitspolitische Interessen, jedoch auch eine kommerzielle Komponente. So seien ausländische Investitionen in Israel ab dem Zeitpunkt in Gefahr, ab dem der Iran über Atomwaffen verfüge und somit Israel als Unternehmensstandort unattraktiver werden ließe, insbesondere für

149 So glauben viele Israelis an den Grundsatz ›*'in every generation they rise against us to destroy us*‹ der Haggada, (zitiert in: Brosgol 2019).

seinen dominanten High-Tech-Sektor, der von ausländischer Finanzierung abhängig ist (Solomon 2012).

Netanjahu positionierte sich in der Iran-Frage bereits früh als Hardliner (›Falke‹),[150] der, falls nötig, mit militärischer Gewalt das Regime in Teheran als Bedrohung ausschalten wollte. Laut Umfragen entsprach diese Position im Jahr 2012 und somit vor dem JCPOA der Mehrheitsmeinung der Israelis (Jerusalem Center for Public Affairs 2012). Das Interesse Netanjahus und der rechts stehenden Likud-Partei an einer gewaltsamen Militäroffensive gegenüber dem Iran äußerte sich Berichten zufolge in zahlreichen internen Auseinandersetzungen mit der Geheimdienst-Community des Landes, die ihre präferierte Strategie der verdeckten Attentate auf Atomwissenschaftler bevorzugte (Bergman 2019, S. 623). Die Geheimdienste und das Militär betrachten den Iran ebenfalls als existenzielle Bedrohung. Gleiches gilt für Teile der moderaten PolitikerInnen Israels (›Tauben‹) wie den früheren Minister- und Staatspräsidenten Schimon Peres (Eiran und Malin 2013, S. 79). Somit lag hier keine Interessensdivergenz vor, sondern eine Unstimmigkeit hinsichtlich der zur Zielerreichung zu präferierenden Mittel.

Dass Netanjahu während der Planungsphase von Stuxnet im Jahr 2007 kein Premierminister war, lässt darauf schließen, dass er hieran nicht unmittelbar beteiligt war. An dieser Stelle kann nicht beurteilt werden, ob sich Israel auch unter seiner Führung seitens der USA zu dieser nicht militärischen Lösung hätte überzeugen lassen können. Netanjahus oftmals geäußerte Präferenz zumindest für die Vorbereitung militärischer Offensiven, aber auch deren letztliche Durchführung (Bergman 2019, S. 623–627), lässt jedoch zumindest Zweifel daran aufkommen. Das Interesse Netanjahus an einer konsequenten, eher militärischen und somit nicht diplomatischen ›Lösung‹ des Iran-Problems belastete besonders dessen Verhältnis zu den USA, insbesondere unter Barack Obama. Auf ideeller und kommerzieller Ebene hatte sich Netanjahu durch den US-Neokonservatismus inspirieren lassen, wodurch sich seine Ablehnung gegenüber dem Oslo-Friedensprozess bei gleichzeitig liberalen Wirtschaftsvorstellungen erklären lässt. Bereits bei seiner Wahl 1996 zum Premierminister wurde dabei jedoch deutlich, dass Netanjahu ideelle Interessen im Zweifel seinem übergeordneten Interesse nach dem eigenen Machterhalt unterordnen würde: So verordnete er der Likud-Partei infolge der Ermordung Rabins eine moderatere Haltung, um den Wahlsieg nicht zu gefährden (Ben-Porat 2005, S. 235). Nichtsdestotrotz war die Präferenzordnung der USA unter Obama, der eine diplomatische Lösung im Umgang mit Teheran vorantrieb, konfliktiver zu der Israels unter Netanjahu als im Falle Bushs. Netanjahu antizipierte wohl dennoch die hohen Kosten, die ein israelischer Militärschlag gegen den Iran während der bereits geführten Vorgespräche zum JCPOA zwischen Washington und Teheran gehabt hätte, da er letztlich darauf verzichtete (Bergman 2019, S. 628). Der israelische Premier manipulierte durch seine ständige Drohkulisse eines Militärschlags das Interdependenzverhältnis zwischen ihm und den USA, was bereits 2007 zur Initiierung von Stuxnet als »*Third Option*« geführt hatte (Perlroth 2021, S. 117).[151] Darüber hinaus versuchte Netanjahu auch, das ›Divided Go-

150 »*It's 1938 (the year before World War II began) and Iran is Germany. And Iran is racing to arm itself with atomic bombs (and) is preparing another holocaust for the Jewish people*«, (Netanjahu 2006, zitiert in: Debusmann 2011).

151 Auch wenn Netanjahu zu diesem Zeitpunkt nicht Premierminister war.

vernment‹ unter Obama zur Opposition gegen das JCPOA auszunutzen und damit eine Asymmetrie auf republikanischer Ebene der USA zu instrumentalisieren (Freedman 2020b). Gleichzeitig hielt das eigene Interdependenzverhältnis zu den USA Netanjahu jedoch davon ab, tatsächlich Krieg gegen den Iran zu führen, da dies zu einem erheblichen Interessenskonflikt mit den Vereinigten Staaten geführt hätte.

Bislang konnte die israelische Regierung kein Interesse daran haben, die israelische Cyberverteidigung generell und insbesondere gegenüber dem Iran als schwach/verwundbar darzustellen, indem öffentlich IT-Operationen fremder Länder im Detail kommentiert/attribuiert wurden. Dies hätte das Offenlegen von Attributionsevidenzen seitens der Geheimdienste erfordert. Netanjahu musste sich nicht zuletzt im Interesse der eigenen Wiederwahl innerhalb der Partei und als Premierminister als ›starker Mann‹ positionieren, der als einziger gegenüber dieser existenziellen Bedrohung für die Sicherheit des israelischen Staates sorgen konnte. Gleichzeitig diente das Durchstechen/Veröffentlichen von Informationen bezüglich vereitelter Angriffe und gelungener Angriffsreaktionen staatlicher Behörden und des Militärs dem israelischen Narrativ der ständigen Bedrohungslage von außen bei gleichzeitig maximaler staatlicher Anstrengung zum Schutz des Landes. Gleiches gilt für die 2012 erstmals öffentlich durch Ehud Barak bestätigte Fähigkeit Israels zur Durchführung offensiver Cyberoperationen, ohne jedoch ins Detail zu gehen (Baram 2017). An dieser Stelle wird eine bedeutende Ambivalenz zwischen der hervorgehobenen iranischen Bedrohung sowie der eigenen (Cyber-)verteidigungs- und (auf Nuklearebene) Zweitschlagfähigkeit sichtbar. Wird Israel als zu stark durch den Iran bedroht und diesem ausgeliefert dargestellt, leidet gleichzeitig dessen Abschreckungspotenzial, wie die Geheimdienste des Landes feststellten (Eiran und Malin 2013, S. 83). Andererseits benötigt der extrem ausgebaute militärisch-industrielle Komplex des Landes, der gleichzeitig sicherheits- sowie wirtschaftspolitischen Interessen dient, ein hinreichend großes Bedrohungsnarrativ für seine Legitimierung.

Solange sich israelische PolitikerInnen somit selbst nicht zu Cyberangriffen auf israelische Ziele äußern bzw. diese eingestehen, können sie nach wie vor ›Plausible Deniability‹ hierüber bewahren. Wie plausibel diese Abstreitbarkeit der eigenen Verwundbarkeit, z.B. im Falle des eigenen Nuklearpotenzials, jedoch noch ist, kann an dieser Stelle kritisch hinterfragt werden. Für israelische AmtsträgerInnen wie Netanjahu galt im Umgang mit dem Iran bislang primär ›Taten, nicht Worte sprechen lassen‹, was sich an den Episoden um Stuxnet sowie den zahlreichen Geheimdienstattentaten auf iranische Atomwissenschaftler ablesen lässt. Das Land verstößt dabei – in Teilen auch gegen den Willen bzw. unter der Maßgabe der ›Plausible Deniability‹ der USA bezüglich der eigenen (Un-)Kenntnis darüber (vgl. Bergman 2019, S. 626) – gegen international anerkannte Normen. Es kann diese Devianzen jedoch verschleiern, indem diesen Normen oftmals selbst gar nicht zugestimmt wurde und zudem über die eigenen Handlungen nicht gesprochen wird. Wenn die eigenen sicherheitspolitischen Interessen in ihrer Durchsetzung denen anderer Demokratien, allen voran der USA, widersprechen, nutzt Israel somit bislang die beschriebene Ambivalenz in unterschiedlichen Bereichen, um diese Konfliktivität der Präferenzordnungen zu verschleiern.

Auch wenn israelische AmtsträgerInnen bislang nicht öffentlich über konkrete Cyberoperationen auf nationale Ziele sprechen bzw. diese attribuieren, liegt eine gänzlich

fehlende Berichterstattung über Cyberangriffe auch nicht im Interesse der Regierung. Indem, wie aufgezeigt, die etablierten israelischen IT-Unternehmen nicht nur öffentlich den Iran und andere Gruppen für Cyberoperationen verantwortlich machen, sondern auch technische Informationen über deren Vorgehen veröffentlichen, stärken diese Threat-Reports die Resilienz israelischer Unternehmen und AkteurInnen. Gleichzeitig müssen durch dieses Verfahren der Mossad oder die Unit 8200 der IDF keine eigenen Attributionsfähigkeiten offenlegen. ›Signaling‹ gegenüber dem Kontrahenten wird bei gleichzeitiger Ambivalenz über die eigenen Kenntnisse und Fähigkeiten gewahrt.

Aufgrund der bestehenden Medienzensur durch das Militär in Israel ist bei den durchgestochenen Details über die israelischen Offensivpotenziale im Cyberspace zudem von bewusst veröffentlichten Informationen auszugehen, um die eigenen Abschreckungspotenziale signalisieren zu können (vgl. Nossek und Limor 2001). Eine mögliche Ausnahme könnten regierungskritischere, säkular-liberal eingestellte Zeitungen wie die Haaretz sein, die nach eigenen Angaben Teil des Investigativjournalismus-Kollektivs war, das 2021 den weltweiten Missbrauch der Pegasus-Spionage-Software der israelischen NSO-Group aufgedeckt hatte. Infolge der Veröffentlichungen geriet Israel unter zunehmenden Druck, die domestischen Spionageunternehmen und deren Exporte stärker zu kontrollieren. Die USA verhängten im Dezember 2021 Sanktionen gegen die NSO-Group sowie das israelische Unternehmen Candiru, woraufhin deren Existenz zum damaligen Zeitpunkt zunehmend gefährdet zu sein schien (Harel und Levinson 2021). Das kommerzielle Interesse Netanjahus, wohl aber auch Naftali Bennets, an ausgeprägten Exporten der israelischen Tech-Industrie auch in autokratische Länder wie Saudi-Arabien führte somit zur Ende 2021 bestehenden Verwundbarkeit der israelischen Branche gegenüber demokratischen Sanktionen, da die kommerziellen Interessen Israels zunehmend in Konflikt zu den ideellen Interessen befreundeter Demokratien gerieten. Die nach den Enthüllungen eingeleiteten Untersuchungen israelischer Behörden gegenüber dem Unternehmen hatten offensichtlich nicht ausgereicht, um aus der kurzfristigen Sensitivität keine Verwundbarkeit für die Branche entstehen zu lassen (vgl. Harel et al. 2021).

Auch für die öffentlichen Attributionen des IT-Sektors gegenüber dem Iran ist im Falle israelischer Ziele von einer Kooperation bzw. zumindest Koordination zwischen dem privaten und öffentlichen Sektor auszugehen. Aufgrund des für Israel noch stärker kolportierten Charakters der ›Revolving Door‹ zwischen staatlichem und kommerziellem Sektor kann diese Annahme wie auch für die USA plausibilisiert werden. Der Gegensatz zwischen dem Veröffentlichen bestimmter Signale und der gleichzeitigen Vermeidung formal-öffentlicher Aussagen hierzu entspricht dem ambivalenten Umgang Netanjahus bei der Bekämpfung des Irans. Aus liberaler Sicht werden somit gleich mehrere Verwundbarkeits-/Informationsasymmetrien manipuliert bzw. verschleiert: die eigene Verwundbarkeit gegenüber iranischen Cyberoperationen, die iranische Verwundbarkeit gegenüber nicht umfassend öffentlich gemachten israelischen Cyberfähigkeiten sowie die Verwundbarkeit Israels im Verhältnis zu den USA. Cyberoperationen wie Stuxnet könnten als eine Art Pendant zu den zahlreichen Tötungen iranischer Atomwissenschaftler gesehen werden, dien(t)en doch beide Maßnahmen dazu, einen offenen militärischen Konflikt zu vermeiden. Beide Strategien sind zudem stärker als Sabotage- denn als Abschreckungsmittel gegenüber dem Iran zu werten (Work und Harknett 2020). Die Be-

reitschaft zur Durchführung von Stuxnet sowie die Fortführung des geheimdienstlichen Anschlagprogramms auch nach dem JCPOA und dessen Aufkündigung durch Donald Trump können somit als Konzessionen Israels gewertet werden, um die eigene Interessensdurchsetzung nicht zu konfliktiv im Verhältnis zu den USA zu gestalten. Auch für Donald Trump war trotz gegensätzlicher Rhetorik ein offener Militärkonflikt mit dem Iran offensichtlich doch kein erstrebenswerter Zustand. So ordnete er offensive Cyberoperationen als Antwort auf iranische Anschläge auf Öltanker in der Straße von Hormus sowie den Abschuss einer US-Drohne 2019 an. Ein Militärschlag als Reaktionsoption war kurzfristig doch noch ausgeschlossen worden (Barnes und Gibbons-Neff 2019).

Die berichtete Episode einer an die Washington Post durchgestochenen Detektion und Attribution einer israelischen Vergeltungs-Cyberoperation gegen den Iran entspricht ferner dem israelischen Interesse, sich nicht selbst für die disruptive Cyberoperation verantwortlich zeigen zu müssen, gleichzeitig jedoch dem Iran und der internationalen Gemeinschaft die eigene Entschlossenheit und ›digitale Zweitschlagsfähigkeit‹ zu signalisieren. Zugespitzt formuliert könnten hier die anonym gebliebenen US-Beamten die Funktion eines defensiven Cyberproxys im Sinne des Signaling erfüllt haben.[152]

In den letzten Jahren zeigt sich jedoch gegenüber der Praxis israelischer Spionagesoftware-Exporte in autokratische Länder, verdeckten ›Extrajudicial Killings‹ und dem eigenen Nuklearstatus, dass diese Ambivalenz besonders seitens domestischer JournalistInnen, aber auch der Zivilgesellschaft stärker kritisiert wird und Rufe nach mehr Transparenz und Offenheit laut werden (Benjakob und Yaron 2021). Die Frage ist, inwiefern für die Regierungen nach Netanjahu die Kosten aus dieser konfliktiven Präferenzordnung zwischen Politik und Gesellschaft so hoch werden, dass die eigene Präferenzordnung verändert werden muss, und welchen Einfluss dies auf den offensiven sowie defensiven Cyberkonfliktaustrag Israels haben wird.

Jüdische Hegemonie in Israel: Ablehnung der Zwei-Staaten-Lösung und jüdische Siedlungspolitik

Als Zweites werden Netanjahus Interesse an jüdischer Hegemonie in Israel und seine damit verbundene, oftmals destruktive Haltung gegenüber dem Friedensprozess sowie einer möglichen Zwei-Staaten-Lösung diskutiert.

Entsprechend der rechts-konservativen Prägung des Likud sowie Netanjahus üben dem Zionismus zugewandte Juden einen erheblichen Einfluss auf deren Politik aus, wenn auch nicht so stark wie ultra-orthodoxe Juden auf noch stärker rechts zu verortende Parteien wie den Ichud Leumi (IL – Nationale Einheit) (Neuberger 2008). Damit verbunden ist das Interesse Netanjahus nach möglichst geringen Konzessionen gegenüber den PalästinenserInnen, etwa in der Frage nach einem Stop oder gar Rückbau der israelischen Siedlungspolitik sowie der offiziellen Anerkennung eines Palästinenser-Staates (Robinson 2020). Gleichzeitig verdeutlicht die Aussage Netanjahus, »*the Palestinians should have the ability to govern their lives but not to threaten ours*« (Benn 2009), dass er kein definitives Nein zur Möglichkeit der Zwei-Staaten-Lösung äußerte, wohl auch, um

---

152 Das berichtete harmonische Verhältnis zwischen Trump und Netanjahu entkräftigt diese Sichtweise zumindest nicht.

nicht zu stark in Opposition zu den am Friedensprozess interessierten USA, vor allem ab 2009 unter Obama, zu treten.[153] Die Interdependenzsituation gegenüber den USA betraf somit nicht nur die Interessensdurchsetzung Netanjahus gegenüber dem Iran, sondern auch in der Palästinenserfrage. Auch hier kann von einer offensichtlich bewusst ambivalenten Haltung Netanjahus im Rahmen seiner Interessensvertretung bzw. deren Kommunikation nach außen gesprochen werden. Die Vermutung liegt nahe, dass dies insbesondere dazu dient, seine zuweilen gegensätzlichen Interessen nach positiven Beziehungen zu den USA sowie seine Verpflichtung gegenüber der Likud-Wählerschaft in Einklang zu bringen bzw. deren Konfliktivität durch die beschriebene Ambivalenz zu manipulieren. Dies entsprach letztlich auch seinem Eigeninteresse des politischen Machterhalts zum Zeitpunkt des genannten Zitats, die bestehende rechts-konservative Koalition nicht durch eine zu moderate Haltung in der Palästinenserfrage zu gefährden.

Im oberen Zitat wird ebenfalls deutlich, dass für Netanjahu die palästinensische Selbstbestimmung nur in dem Rahmen möglich ist, in dem diese die Ausbreitung und Entfaltung jüdischen Lebens in Israel nicht behindert. Daher wird dieser Abschnitt auch als Netanjahus Interesse nach ›jüdischer Hegemonie in Israel‹ bezeichnet. Dieses Interesse kulminierte 2018 im bereits genannten ›Basic Law: Israel – The Nation State of the Jewish People‹, das aus Sicht vieler BeobachterInnen zu einer Degradierung in Israel lebender Muslime gegenüber Juden führte (z.B. Jabareen und Bishara 2019). Darin wurde u.a. konstatiert, Israel sei »*the national home of the Jewish people*« (Jabareen 2018). Des Weiteren wurden die 1967 eroberten Teile des historischen Palästinas offiziell als Teil des israelischen Staatsterritoriums anerkannt, somit de facto annektiert. Aufgrund dieser Bezüge zu geografischen Grenzen, nationalen Identitäten sowie Vorstellungen darüber, welche Gruppierungen von welchen sozio-ökonomischen Privilegien im Staatsgebiet besonders profitieren sollten, handelt es sich hierbei um ein prävalentes Interesse auf ideeller Ebene. Netanjahu wurde zugleich der Vorwurf gemacht, er habe damit der religiösen Identität den Vorzug vor Israels Identität als liberaler Demokratie gegeben (Khan 2018).

Das Interesse nach jüdischer Hegemonie in Israel betrifft jedoch auch die kommerzielle Ebene des Liberalismus, wobei zwei Befunde der Forschung besonders herausstechen: Erstens wurden Netanjahu zumindest auf wirtschaftlicher Ebene durchaus erfolgreiche Maßnahmen bescheinigt, um den Status der PalästinenserInnen zumindest aus sozio-ökonomischer Sicht zu verbessern (Freedman 2020a, S. 4). Es kann also von einem Interessenskonflikt Netanjahus auf ideeller vs. kommerzieller Ebene gegenüber den PalästinenserInnen gesprochen werden, wobei er offensichtlich den Mehrwert entsprechend ausgebildeter und an der israelischen Wirtschaft beteiligter PalästinenserInnen erkannte.

153 Der vorläufige Höhepunkt des Dissents zwischen Netanjahu und Obama bestand im nicht eingelegten Veto der USA gegenüber einer UN-Resolution 2016, die die israelische Siedlungspolitik verurteilte (Beaumont 2016). Dass die USA auch unter Obama jedoch in Form von langjährigen Zusagen für Waffenlieferungen israelischen Sicherheitsbedürfnissen entsprochen haben Freedman 2020b, verdeutlicht, dass auch innerhalb der Palästinenserfrage zuweilen unterschiedliche Subinteressen auf ideeller vs. wirtschaftlicher Ebene zu varianten Policies führen können.

Zweitens ist auf kommerzieller Ebene der ›Pivot to Asia‹ unter Netanjahu zu nennen: Infolge vermehrter europäischer Kritik an der israelischen Siedlungspolitik orientierte sich die israelische Industrie immer stärker Richtung Asien und erschloss die dortigen Märkte (Inbar 2020). Die ideelle Interessensdurchsetzung Netanjahus führte somit zu einem Interessenskonflikt mit europäischen Ländern, der jedoch nicht zu einer längerfristigen wirtschaftlichen Vulnerabilität Israels aufgrund entgangener europäischer Wirtschaftsaufträge führte, da als Ausgleich alternative Absatzmärkte in Asien erschlossen werden konnten.

Auf ideeller Ebene verband Netanjahu sein Interesse an einer kompromisslosen Haltung gegenüber den PalästinenserInnen auch mit dem an einer Einhegung des Irans und dessen Proxys (z.B. Hisbollah). Da laut Umfragen im Jahr 2012 eine Mehrheit der befragten Israelis die Meinung äußerte, dass der iranische Besitz von Atomwaffen die Hisbollah sowie die palästinensische Hamas gefährlicher werden lasse, entsprach die Sekuritisierung palästinensischer Souveränitätsbestrebungen, insbesondere in Verbindung mit der Hamas, auch der Mehrheitsmeinung der Israelis, zumindest zum damaligen Zeitpunkt (Jerusalem Center for Public Affairs 2012).

Im Folgenden wird dargestellt, welche Aspekte der israelischen Politik im Rahmen von Cyberkonflikten sowie der beschriebenen Attributionen des IT-Sektors sich hierdurch erklären lassen. Als erster empirischer Fall kann die 2019 erfolgte, erstmalige israelische Militäroperation als Antwort auf einen Hackerangriff der Hamas genannt werden: Anfang Mai hatten die IDF ein Gebäude im Gaza-Streifen bombardiert, in dem sich laut israelischen Angaben die Cyberzentrale der Hamas befunden hatte, wovon zuvor zahlreiche Cyberangriffe auf Israel ausgegangen seien (Cimpanu 2019). Dabei werteten die israelischen Stellungnahmen zum Vorfall die Cyberfähigkeiten der Hamas im Gegensatz zur eigenen Überlegenheit rhetorisch ab. Israel bediente sich hier somit derselben ambivalenten Strategie wie im Falle der Stilisierung des Irans als existenzieller Bedrohung: Wenn die Cyberangriffe der Hamas so ungefährlich und rudimentär waren, stellt sich die Frage, warum Israel sogar mit militärischen Mitteln hierauf antwortete. Die proaktiven Aussagen offizieller Stellen zur Operation stellen eine ähnliche Abkehr von der sonstigen Verschwiegenheit dar, wie im Falle der generalisierten ›Quasi-Attributionen‹, dass tägliche Angriffe von Ländern wie dem Iran erfolgten, jedoch keine konkreten Details preisgegeben werden.

Aus völkerrechtlicher Sicht ist die Angemessenheit dieser Reaktion durchaus umstritten, von israelischer Seite aus handelte es sich dabei um Anti-Terror-Maßnahmen bzw. unerlässliche Handlungen zum Schutze Israels, ähnlich wie bei Extrajudicial Killings, Stuxnet sowie dem eigenen Atomwaffenprogramm.[154] Hinzu kommt, dass sich die Hamas offiziell auf israelischem Boden befand und somit keine Souveränitätsverletzung eines anderen Landes für das Manöver in Kauf genommen werden musste, was es für Israel wohl weniger brisant und die Hacker (auch offiziell) zu legitimen Zielen machte (Newman 2019).

154 Israel begann jedoch bereits in den 1970-er Jahren auch mit solchen gezielten Tötungen feindlicher PalästinenserInnen im Gaza-Streifen und damit einem von Israel kontrollierten Gebiet, anstatt diese Personen entsprechend völkerrechtlicher Bestimmungen im Zuge eines Gerichtsverfahrens zu belangen (Bergman 2019, S. 134).

Der Fall ist besonders aufschlussreich hinsichtlich der Analyse der IV für Israel unter Netanjahu: Die Einbettung attribuierter Cyberoperationen in einen gewaltsamen Konflikt mit der Partei der CyberangreiferInnen (Hamas) ließ erstens nicht nur die sonstige Attributionszurückhaltung Israels in diesem Falle schwinden, sondern es wurde zweitens hierdurch sogar eine militärische Eskalationshandlung legitimiert. Der Fall wurde nicht über IT-Unternehmen attribuiert, da eine (sichtbare) militärische Gegenmaßnahme durch die eigene, zumindest politische ›Quasi-Attribution‹ der Cyberangriffe der Hamas gerechtfertigt werden sollte. Dass die Cyberoperationen der Hamas laut IDF-Angaben zudem wie viele weitere auch vereitelt werden konnten und dennoch mit einem Luftschlag darauf reagiert wurde (Cimpanu 2019), nährt weiter die Zweifel an der rechtlichen Legitimation der Handlung. Auch hier bediente sich Israel einer ambivalenten Attributions- und Kommunikationsstrategie: Gegenüber einem allgemein existenzbedrohenden Akteur wurden extreme militärische Maßnahmen gerechtfertigt, der konkrete Fall wurde jedoch als ungefährlich bzw. durch die IDF vereitelt dargestellt. Wie für die übrigen israelischen ›Quasi-Attributionen‹ wurden keine technischen Evidenzen präsentiert. Für die hiermit verbundene Attributionsfunktion der Rechtfertigung militärischer Maßnahmen erschien dies aus israelischer Sicht nicht notwendig, da die unbestrittene Gefahr der Hamas auf konventioneller Ebene auf deren Cyberverhalten übertragen wurde. Im Verbund mit der von US-Offiziellen durchgestochenen Attribution einer israelischen Cybervergeltung gegen den Iran spricht diese Episode dafür, dass militärische Konflikte als Ausprägung der IV zumindest eine partielle Aufgabe der ansonsten dominierenden Attributionszurückhaltung und Verantwortungszuweisung via IT-Unternehmen in Israel bewirken.

Bereits 2016 wurde zudem Anklage gegen einen besonders versierten Hacker der Terrorgruppe ›Palestinian Islamic Jihad‹ erhoben. Maagad Ben Juwad Oydeh hatte zuvor jahrelang israelische Ziele, darunter die Aufnahmen unbemannter Drohnen der IDF, die über den Gaza-Streifen flogen, weiterer Überwachungskameras des Militärs und der Polizei sowie einen Flughafen gehackt. Berichten zufolge stand Oydeh in Kontakt mit dem Iran und sollte dort weiter ausgebildet werden, was letztlich nicht zustande kam (Bob 2016). Im Gegensatz zur US-Strategie ›Attribution by Indictment‹ befand sich Oydeh jedoch zum Zeitpunkt der Anklage bereits in Haft. Hierbei stand somit der strafrechtliche Aspekt der Anklage und weniger dessen Signaling-Funktion im Vordergrund. Auch dieser Fall verdeutlicht aus israelischer Sicht die Verbindung zwischen dem Iran und palästinensischen ExtremistInnen als Bedrohung.

Aufseiten der technischen Attributionen israelischer Unternehmen lassen sich durch das Interesse Netanjahus an jüdischer Hegemonie somit grundlegend auch die erfolgten Attributionen gegenüber AngreiferInnen mit palästinensischer Herkunft plausibilisieren. Wie Abbildung 35 zeigt, erfasst der HD-CY.CON israelische IT-Unternehmen erst ab 2012 als Attributionsquellen. Dies korrespondiert einerseits mit der generellen Entwicklungsgenese der Branche, hängt andererseits wohl jedoch auch mit der nach der Stuxnet-Enthüllung für Israel allgemein gesteigerten Bedrohungslage im Cyberspace zusammen. Die seit 2012 erfassten Cyberoperationen mit attribuiertem Country-Code ›PSE‹ auf der Angreiferseite gegen israelische Ziele (n = 11) verdeutlichen, dass sich diese Gefahr nicht nur auf den Iran beschränkte. Dies erklärt auch die fünf verzeichneten Attributionen israelischer IT-Unternehmen in Richtung palästinensischer AkteurInnen

(Abbildung 37). Der 2019 erfolgten Militärreaktion auf die Cyberzentrale der Hamas war der erste Raketenbeschuss Israels aus dem Gaza-Streifen seit 2014 vorausgegangen. Dies indiziert, dass für die israelische Attributionspolitik besonders die jeweilige Konflikt-Situation eine Rolle spielt und bereits erfolgte Eskalationen zu reduzierten Attributionen via Proxys führen.

5.7.3.3 Die israelische Geheimdienst-Community: Politik als Fortführung des militärischen Kampfes, jedoch mit verdeckten Mitteln

Auch wenn die israelischen Geheimdienste grundlegend die beiden oben genannten Interessen Netanjahus teilen, werden in diesem Abschnitt Differenzen zwischen politischer und geheimdienstlicher Ebene identifiziert und im Sinne der Proxynutzung diskutiert.

Wie Ronen Bergman in einer der wenigen umfassenden Abhandlungen über die israelischen Geheimdienste 2019 darlegte, sind die israelischen Geheimdienste Shin Bet, Mossad sowie die IDF eng mit der historischen Genese Israels verbunden. Aus früheren UntergrundkämpferInnen im britischen Mandatsgebiet Palästina wurden später führende Beamte staatlicher Einheiten des jungen Staates, die dessen Sicherheitspolitik gegenüber ausländischen und inländischen Bedrohungen prägten. Aufgrund des permanent aktivierten Überlebensmodus Israels entwickelte sich der beschriebene militärisch-industrielle Komplex in seiner heutigen Form und verschaffte militärischen sowie zivil-geheimdienstlichen Stellen einen exponierten Zugang zu politischen EntscheidungsträgerInnen. Wie aufgezeigt, wurde jedoch infolge der politischen Reformen Ende der 1990er Jahre vor allem die Stellung des Premierministers gestärkt. Dass dieser »das letzte Wort« gegenüber den Geheimdiensten hat, betont auch Bergman (2019, S. 628).

Netanjahus Beziehung zu den Geheimdiensten, allen voran dem früheren Mossad-Chef Dagan Meir, wird als weitaus konfliktiver bezeichnet als die früherer Premierminister (vgl. Bergman 2019, S. 623). So kam es zu einer grundlegenden Opposition der Geheimdienste gegenüber Netanjahu in vielen strategischen Fragen. Dies betraf weniger grundlegende Zielkonflikte als die zu deren Erreichung einzusetzende Mittelauswahl. So berichtet Bergman über Dagan Meirs Disput mit Netanjahu hinsichtlich des richtigen Vorgehens gegenüber der iranischen Nuklearbedrohung: Während Netanjahu auf einen Militärschlag bzw. dessen Androhung pochte, beurteilte Dagan einen Militärkonflikt mit dem Iran als fatal für das israelische Interesse an Stabilität und Sicherheit in der Region (Bergman 2019, S. 623).

Auch kurz vor dem Ende seiner Zeit als Premierminister stellte Netanjahu aus Sicht der Geheimdienste zu häufig sein politisches Eigeninteresse vor das nationale Interesse an politischer Stabilität, wie die Kritik des früheren Shin-Bet-Chefs Nadav Argaman im Juni 2021 an den seitens der Likud-Partei angefachten Protesten im Kontext der bevorstehenden Regierungsbildung zeigte (Kingsley 2021). Andererseits waren die Geheimdienste aufgrund der bestehenden Informations- und Berichtskette direkt an Netanjahu in Teilen auch gezwungen, diesem bei seinen politisch motivierten Schachzügen gegen KontrahentInnen wie Benny Gantz zu helfen. So wurde 2019 bekannt, dass der iranische Geheimdienst das Telefon von Gantz gehackt und kompromittierende Dateien erlangt habe. Die israelischen Geheimdienste hatten dies Gantz noch vor dem Öffentlichwerden des Hacks mitgeteilt und, im Zuge der bestehenden Befehlskette, vermutlich auch

Netanjahu (Der Spiegel 2019). Die Betonung des Irans und dessen Proxys als zentraler Gefahr für Israel durch den 2021 eingesetzten Shin-Bet-Chef Ronan Bar verdeutlicht jedoch, dass auch über Netanjahus Amtszeit hinaus Interessenskonvergenz zwischen der politischen sowie militär-geheimdienstlichen Ebene in außenpolitischen Fragen zu existieren scheint (Bob 2021).

Aus zeitlicher Sicht hatten insbesondere die Ermordung von Jitzchak Rabin 1995 sowie der 11. September 2001 einen Einfluss auf die israelische Geheimdienstarbeit. Diese beiden »*Intelligence-Blunders*« führten auch in Israel zu einer stetigen Ausweitung der eigenen Cyberspionage- sowie Cybersicherheitskapazitäten, was wiederum den heimischen IT-Sektor stärkte (Moersen 2018).

Aufgrund der Interessenskonvergenz zwischen Netanjahu und den Geheimdiensten sowie dessen letztlicher Oberbefehlsgewalt erklärt primär die von Bergman 2019 beschriebene Präferenz der Geheimdienstcommunity für verdeckte Operationen Teile des israelischen Cyberkonfliktaustrags. Dabei geht es weniger um deren inhaltliche Ausrichtung als um deren Form. Dass Israel sich offiziell nur in den beschriebenen Einzelfällen zu eigenen Cyberoperationen bekannt hat, entspricht der Ambivalenz zwischen angestrebter Geheimhaltung und gleichzeitiger Signalisierung der eigenen Fähigkeiten. So wie dem Iran durch die Ausschaltung dessen Nuklearwissenschaftler die Verwundbarkeit gegenüber israelischen Geheimdienstoperationen signalisiert werden sollte, wurde ein solches Signaling zumindest partiell auch gegenüber AngreiferInnen im Cyberspace angestrebt. Da Cyberoperationen oftmals noch schwieriger zu detektieren sind als Attentate, war diese Quasi-Selbstattribution hierfür nötig. Ein weiteres historisches Beispiel dieser ambivalenten Verschleierungsstrategie der israelischen Geheimdienste gegenüber der Bevölkerung ist deren Umgang mit Terroranschlägen der Fatah im 20. Jahrhundert: Um der aufstrebenden Bewegung keine öffentliche Anerkennung für ihre Taten zukommen zu lassen, wurden diese jahrzehntelang nur als »*hostile terrorist activity*« bezeichnet, ohne namentliche Nennung der Gruppe (Bergman 2019, S. 113).

Ein Beispiel für einen Interessenskonflikt zwischen politischer Führung und den Geheimdiensten nach dem bis heute relevanten Sechs-Tage-Krieg 1967 wird jedoch im Buch von Ronan Bergman beschrieben: So sprach sich der damalige AMAN-Forschungsleiter Gazit in einem internen Papier für einen moderateren Umgang mit den besiegten arabischen Staaten aus, um eine endgültige Befriedung des Konfliktes herbeizuführen. Damit verbunden forderte er als israelische Gegenleistung für einen Friedensdeal den partiellen Rückzug aus den eroberten Gebieten sowie die Errichtung eines unabhängigen Palästinenserstaates (Bergman 2019, S. 114). Zumindest der AMAN präferierte in diesem Fall somit das Interesse an langfristigem und belastbarem Frieden für Israel vor dem Interesse an jüdischer Hegemonie gegenüber den Palästinensern. Die politische Führung sah dies damals jedoch anders, genauso wie Netanjahu in jüngerer Zeit aus Sicht der Geheimdienste und aus politischem Eigeninteresse zu eskalativ gegenüber dem Iran und Palästina agierte.

Grundlegend etablierte sich in Israel auf politischer Ebene die Haltung, dass verdeckte Operationen nicht nur ein taktisches, sondern auch ein strategisches Mittel sein könnten. Teile der hierfür durch jahrzehntelange Geheimoperationen verantwortlichen Dienste erkannten laut Bergman den Trugschluss dieser Annahme jedoch selbst: So könnten Attentate und wohl auch Cyberoperationen politischen Dialog nicht ersetzen,

was auch die zahlreichen Misserfolge solcher Operationen demonstrierten (Bergman 2019, S. 630).

Für den offensiven Cyberkonfliktaustrag Israels sowie dessen Umgang mit der öffentlichen Detektion und Attribution fremder Cyberangriffe wird somit in Zukunft auch die Haltung der Geheimdienste entscheidend sein. Das Beispiel der NSA unter Anne Neuberger deutet dabei an, dass Personen einen Unterschied machen können und bestehende Geheimhaltungstraditionen in Institutionen zu Gunsten verstärkter Informationsweitergabe auch an den Privatsektor im Rahmen von VEPs aufweichen können.

5.7.3.4 Die israelische Rüstungs- und Cybersicherheitsindustrie zwischen Patriotismus und internationalem Kundenprofil

Zuletzt gilt es die genuinen Interessen des israelischen Rüstungs- und Cybersicherheitssektors differenzierter zu betrachten, auch wenn dieser eng mit der militärisch-geheimdienstlichen Ebene verwoben ist. Letztlich befinden sich beide Seiten in einer symbiosehaften Koexistenz: Der Militärsektor lebt von den Innovationen der Tech-Industrie, letztere von den Aufträgen des Militärs und des Staatsapparats sowie dessen politischer Unterstützung ausländischer AuftraggeberInnen. Für beide Seiten ist die Ambivalenz zwischen der Aufrechterhaltung des Narrativs der ständigen Bedrohung Israels sowie der Betonung der eigenen Kapazitäten und Fähigkeiten unabdingbar. Daraus ergibt sich wie für das Militär ein privatwirtschaftliches Interesse an der Bekämpfung des Irans sowie einer nicht nur politischen Konfliktbearbeitungsstrategie gegenüber den PalästinenserInnen. Gleichzeitig treten Militär und Privatwirtschaft, wie beschrieben, immer stärker in Konkurrenz um die größten Talente im IT-Bereich. Durch die allgemeine Wehrpflicht als erster Station, den danach oftmals erfolgenden Wechsel in die Industrie sowie den jährlich abzuleistenden Militärreservedienst ist dennoch eine gegenteilige Vorteilsnahme in gewisser Weise garantiert (Herpig et al. 2020, S. 6). Gleiches gilt für öffentliche Schnittstellenprojekte zwischen Industrie und öffentlichem Sektor wie dem genannten ›Israeli Cyber Company Consortium‹. Dieser letzte Aspekt könnte erklären, warum sich AkteurInnen aus israelischen Sicherheitskreisen infolge der Pegasus-Enthüllungen und der damit verbundenen US-Sanktionen gegen die NSO-Group anonym in Zeitungen mit der Aussage zitieren ließen, dass die NSO-Group aus eigenem Interesse gegenüber den USA hätte verteidigt werden sollen (Bar-eli 2021). Es deutet sich hier eine auf BeamtInnen-Ebene bestehende Präferenz für die Interessen des militärisch-industriellen Komplexes gegenüber dem Interessensausgleich mit liberal-demokratischen Ländern aufgrund der Pegasus-Affäre an.

Grundlegend können die wirtschaftlichen Interessen des israelischen Rüstungs- und Cybersektors deren immer größere Involvierung im öffentlichen Attributionsprozess erklären. Es werden immer wieder neue IT-Unternehmen gegründet, die sich ebenfalls daran beteiligen.[155] Aus inhaltlicher Sicht wurde bereits der dualistische Charakter der Attributionen angesprochen: Diese fokussieren sich einerseits auf israelische Ziele betreffende AngreiferInnen, andererseits jedoch auch auf internationale Ziele, z.B. Cyberspionageoperationen aus China oder anderen Ländern. Beides entspricht den Interes-

155 So ist das noch unbekanntere Unternehmen ›Security Joes‹ laut eigener Website erst seit Anfang 2021 im Threat Research Bereich aktiv (Security Joes 2021).

sen der Unternehmen: Durch den Fokus auf israelische Ziele wird die eigene Legitimation als potenzieller Proxy des Heimatstaates unter Beweis gestellt, von dessen Aufträgen und Unterstützung die Branche massiv profitiert. Andererseits wird der stetig wachsende Kundenstamm auf internationaler Ebene durch technische Attributionsberichte besser über die wachsenden Gefahren proliferierender Angriffstechniken informiert. Dass es im Gegensatz zu den USA noch zu keiner intensiven öffentlichen Auseinandersetzung mit chinesischer Wirtschaftsspionage gegen israelische Unternehmen gekommen ist, könnte dabei an zwei Umständen liegen: Erstens könnte Israel entsprechend seiner generell stärkeren (öffentlichen) Attributionszurückhaltung den nichtöffentlichen Attributions- und Signalingkanal über diplomatische Kanäle gegenüber Peking bevorzugen. Zweitens könnten die eigenen wirtschaftlichen Interessen gegenüber der VR China die israelische Regierung vor einer öffentlichen Attribution zurückschrecken lassen (vgl. Tress 2021). Besonders der Fall von chinesischer Cyberspionage gegen drei führende israelische Rüstungsunternehmen zwischen 2011 und 2012 ist hier von Interesse: Dabei wurden sensible Daten des Raketenabwehrsystems Iron Dome gestohlen, das insbesondere während des Raketenbeschusses aus dem Gaza-Streifen 2021 als israelische Erfolgsgeschichte gefeiert wurde (Krebs 2014). Vermutlich berichteten gerade deshalb israelische IT-Unternehmen nicht über den Fall, von dem gerade sie in der Branche zuerst erfahren haben dürften. Stattdessen brachte ein US-IT-Unternehmen (CyberESI) gemeinsam mit dem IT-Journalisten Brian Krebs den Vorfall an die Öffentlichkeit. Eine technische Detektion und Attribution lagen hier wohl eher nicht im israelischen Interesse, da dies auf einen potenziellen Sicherheitsvorfall und damit die eigene Verwundbarkeit gegenüber fremdländischer Cyberspionage aufmerksam gemacht hätte. Hinzu kommt der erwähnte ›Pivot to Asia‹ Netanjahus, der ebenfalls zu einer auch politischen Attributionszurückhaltung in diesem Fall geführt haben dürfte.

Zusammengefasst besitzen israelische IT-Unternehmen ein großes Eigeninteresse daran, ihre Fähigkeiten im Threat-Research-Bereich auch durch öffentliche Attributionen zu demonstrieren. Die im HD-CY.CON erfasste technische Berichterstattung auf Ziele in Israel sowie seitens iranischer und palästinensischer AngreiferInnen im Allgemeinen liegt auch im Interesse der israelischen Regierung, um die Resilienz der anvisierten Ziele zu stärken. Gleichzeitig mussten durch die stellvertretenden technischen Attributionen der Mossad sowie die Unit 8200 jedoch keine eigenen Attributionsfähigkeiten offenlegen. Unklar bleibt an dieser Stelle, inwiefern zumindest manche der kolportierten Frontunternehmen des Militärs, auch aufgrund der rechtlichen Grauzone bezüglich ›aktiver Cyberverteidigung‹, auch als offensive Cyberproxys bezeichnet werden könnten: Indem Unternehmen unterhalb der kritischen Schwelle des ›Use of Force‹ in gewissem Maße Hack-Backs erlaubt werden, könnten diese bewusst in die staatliche Cyberoffensive integriert werden (vgl. Herpig et al. 2020, S. 6).

5.8 Amerikanische und israelische Cyberproxy-Nutzung im Vergleich

Wie für die beiden Autokratien werden die zentralen Befunde der demokratischen Fallstudien hinsichtlich der aufgestellten Hypothesen vergleichend gegenübergestellt.

Die Analyse der zentralen Interessensgruppen im US-amerikanischen und israelischen politischen System verdeutlichte das Interesse beider Länder an privatwirtschaftlichen Attributionen im Cyberspace. Weder die USA noch Israel zeigten im Untersuchungszeitraum eine konsequente, öffentlich-politische Attributionsstrategie, die technische Verantwortungszuweisungen obsolet gemacht hätte. Auch wenn sich die USA unter Trump weitaus proaktiver hinsichtlich der Beschuldigung autokratischer CyberangreiferInnen zeigten, besonders im Zuge öffentlicher Anklageerhebungen, waren diese Attributionen doch eher punktueller Natur, unterschiedlich hinsichtlich ihrer jeweiligen Veröffentlichungsform und auch der dabei präsentierten Attributionsevidenzen. Israel zeigte dagegen eine generelle Attributionszurückhaltung der Regierung und politischer AkteurInnen, die allenfalls einzelne Quasi-Attributionen zuließ. Für beide Länder dominierten zahlenmäßig technische Attributionen nationaler IT-Unternehmen, für die unterschiedliche Proxy-Funktionen entsprechend der Ausprägungen der AV plausibilisiert werden konnten. Möglich machten dies die Stellung und Entwicklung der heimischen Tech-Industrie sowie deren enge Beziehungen zum öffentlichen Sektor (›Revolving Door‹; KV).

Beginnend mit den Hypothesen über das Wirken der UV auf die beiden AVs lässt sich Folgendes feststellen: Wie durch H1 behauptet,[156] wurden in der Tat sowohl für die USA als auch Israel insbesondere dann unterschiedliche Proxy-Funktionen festgestellt, wenn die eigene Verwundbarkeit gegenüber offensiven Cyberoperationen autokratischer Staaten besonders groß war. Zurückgeführt wurde dies für die USA auf wirtschaftliche Präferenzinkompatibilitäten mit China sowie stärker ideelle Präferenzinkompatibilitäten gegenüber Russland als Kontrahenten im Cyberspace. Die umfassende Wirtschaftsspionage chinesischer CyberangreiferInnen nutzte die bestehende Verwundbarkeit der US-Wirtschaft aufgrund mangelnder IT-Sicherheit und zugleich vorhandenen geistigen Eigentums aus. Russland verschärfte dagegen insbesondere im Zuge der Präsidentschaftswahlen 2016 den aufgrund steigender Polarisierung bereits vor der Wahl Trumps sich abzeichnenden Illiberalisierungsprozess der USA, indem durch die gezielten Hack-and-Leak-Operationen sowie Fake-News-Kampagnen der Wahlprozess als ideeller Kern liberaler Demokratien unterminiert wurde.

Für Israel konnte dagegen ein eingeschränkteres Funktionsprofil der technischen Proxys aufgezeigt werden: So waren deren Attributionen primär auf das stellvertretende öffentliche Signaling gegenüber CyberangreiferInnen wie dem Iran oder palästinensischen HackerInnen sowie die Schaffung technischer Resilienz durch die Veröffentlichung technischer Indikatoren ausgerichtet. Es kam (außer in dem berichteten Fall der jedoch vereitelten Cyberspionage-Operation von Lazarus 2020) zu keiner Sequenzierung technischer und öffentlicher Attributionen, wie sie für die USA in den behandelten Fallbeispielen der Anklage aus 2014 (APT1 Report) sowie dem DNC-Hack diskutiert wurde. Stattdessen legte Israel auch bezüglich der öffentlichen Kommentierung von eigenen sowie fremden Cyberoperationen eine bemerkenswerte Verschwiegenheit an

156 H1 (UV): Je umfassender die eigenen Verwundbarkeiten im Rahmen konfliktiver Präferenzinkompatibilitäten zu anderen Staaten auf einer oder allen drei Liberalismus-Ebenen durch offensive Cyberoperationen ausgenutzt werden, desto größer sind die demokratischen Anreize für die Nutzung defensiver Cyberproxys.

den Tag, die lediglich von punktuellen, wenig detailreichen Signaling-Äußerungen durchbrochen wurde. Da sich die technischen Attributionen israelischer Unternehmen besonders auch auf iranische und palästinensische Operationen fokussierten, AkteurInnen, deren Angriffe sowohl auf der konventionellen als auch Cyber-Ebene israelische Verwundbarkeiten besonders betrafen, kann auch für Israel die H1 weitgehend bestätigt werden. Gleiches gilt für den israelischen Umgang mit chinesischen Cyberspionageoperationen, die offensichtlich als geringere Gefahr für die eigenen Wirtschaftsinteressen angesehen wurden, als für die USA unter Obama.

Diese Ausführungen deuten bereits die Erklärungskraft der H2 an:[157] So bewerteten die USA und Israel offensichtlich nicht dieselben Cyberproxy-Funktionen ihrer IT-Unternehmen als besonders nützlich im Sinne ihrer eigenen Interessensdurchsetzung. Für Israel stand das Signaling gegenüber politischen Kontrahentinnen und weniger die Legitimation politischer Attributionen durch IT-Unternehmen im Vordergrund, da Letztere für die präferierte Strategie verdeckter Beantwortungsoptionen noch weniger benötigt wurden als für öffentliche Maßnahmen. Der Fall des Militärschlags gegen die Hamas-Cyberzentrale zeigt jedoch, dass in diesem Fall zumindest eine generische Quasi-Attribution staatlicher Stellen vorgenommen wurde, da es sich hierbei um eine notwendigerweise öffentlich sichtbare und zudem gewaltsame Reaktion handelte.

Aufgrund des Wirkens unterschiedlicher Verwundbarkeitsasymmetrien kam es in den USA besonders unter Obama und Trump zu einer varianten Attributionspraxis, die unter Trump noch stärker den auch im Offensivbereich propagierten ›Defending-Forward‹- und ›Persistent-Engagement‹-Ansätzen entsprach. Grundlegend gab es für die konzeptualisierte Staat-Proxy-Beziehung während Trumps Präsidentschaft weniger Evidenzen als für die Obama-Ära, veranschaulicht an den beiden Fallbeispielen des APT1-Berichts und des DNC-Hacks. Entsprechend Trumps Abneigung gegenüber liberal-demokratischen Prinzipien auf ideeller Ebene wie Multilateralismus oder der Propagierung rechtstaatlicher Prinzipien, verband er seine proaktivere Attributionspolitik nicht mit der Forcierung eines breiten demokratischen Attributionsbündnisses, das auf vorab etablierten Völkerrechtsprinzipien für den Cyberspace basierte, sondern wählte entsprechend seiner Selbstperzeption als ›Deal-Maker‹ fallabhängige Attributionsallianzen aus. Ebenso etablierte die prävalente Form der Selbstattribution durch anonyme US-Quellen in Medienberichten weder rechtstaatliche noch völkerrechtliche Prinzipien im Umgang mit eigenen Offensivoperationen im Cyberspace und letztlich auch keinen demokratischen Normaufbau in diesem Bereich.

Zuvor hatte Barack Obama aufgrund des steigenden politischen Drucks der Wirtschaft sowie des damals republikanisch geführten Kongresses erstmals private Attributionsberichte in die politische Strategie gegenüber China als Kontrahenten im Cyberspace integriert. Die Anklage von 2014, die sich auf Evidenzen des APT1-Berichts von Mandiant stützte, erhöhte den politischen Druck auf Peking und führte schließlich zum Abschluss des Obama-Xi-Abkommens 2015. Aufgrund Obamas Präferenz für Multilateralismus sollte dieses erste bilaterale Abkommen wohl auch den Grundstein für einen

157 *H2 (UV): Je größer der erwartete Nutzen bestimmter Formen defensiver Cyberproxy-Funktionen zur Reduzierung eigener Verwundbarkeiten auf ideeller, wirtschaftlicher sowie republikanischer Ebene ist, desto wahrscheinlicher ist deren Anwendung seitens der jeweiligen Demokratie.*

internationalen Normbildungsprozess bilden, der sich in weiteren Abkommen wie zwischen China und Großbritannien zumindest auch angedeutet hatte.

Dass sich das Verhältnis zwischen den USA und China nach Trumps Wahl nicht nur im konventionellen Bereich verschlechterte, lag an der zunehmend konfliktiven Präferenzkonstellation der beiden Länder auf kommerzieller Ebene. Dass für Trumps Amtszeit jedoch nur in zwei Fällen sowohl technische als auch politische Attributionen gegenüber chinesischen Cyberoperationen mit staatlicher Beteiligung erfasst wurden, spricht dafür, dass im Umgang mit China aus Sicht der Trump-Administration die konventionellen Konfliktaustragungsmittel wie Sanktionen im Mittelpunkt standen. Dass auch die Trump-Administration verstärkte Attributionen staatlicher AkteurInnen in Richtung autokratischer Regime nichtsdestotrotz als nützlich erachtete, indizieren auch die eingesetzte Cyber Solarium Comission sowie die Gründung der CISA. Der Konflikt um die Behauptung der Trump-Administration vor der Wahl 2020, nicht Russland sei die Hauptbedrohung im Cyberspace, sondern China und der Iran, der die Geheimdienstcommunity widersprach (Marquardt et al. 2020), verdeutlicht jedoch sowohl den Einfluss des Subregimetypus auf das Verhalten demokratischer Staaten im Cyberspace als auch die Prävalenz des Eigeninteresse Trumps für dessen politische Entscheidungen. Gleiches gilt für die Aussage des CISA-Leiters Chris Krebs, die Wahlen 2020 seien sicher gewesen, weshalb er von Trump entlassen wurde. Im Gegensatz zu Netanjahu konnte Trump sich jedoch nicht in den meisten Fragen auf eine breite Mehrheit der Bevölkerung stützen, die seine Ansichten teilte, weshalb im Falle der USA auch von noch stärkeren Differenzen zwischen dem Sicherheitsapparat und dem Präsidenten berichtet wurde. Insbesondere die Interessenskonstellation zwischen Regierung, Militär/Geheimdiensten, Tech-Industrie sowie dem Selektorat ist in Demokratien mitentscheidend für die öffentliche Attributionspolitik und Cyberproxy-Nutzung. Im Falle der USA unter Trump herrschte im Gegensatz zu Israel unter Netanjahu nicht nur ein Dissens bezüglich der einzusetzenden Mittel zur Erreichung eines gemeinsamen Ziels, sondern es bestanden grundlegende Interessenskonflikte zwischen weiten Teilen der Bevölkerung und dem Staatsapparat auf der einen sowie dem Trump-Lager und dessen AnhängerInnen auf der anderen Seite.

Die Befunde deuten für die USA unter Trump jedoch auch eine eingeschränktere Erklärungskraft der H1 an, da trotz der Präferenzinkompatibilitäten gegenüber China auf wirtschaftlicher Ebene offensichtlich nicht verstärkt auf Cyberproxys gesetzt wurde. Je illiberaler eine Demokratie wird, desto weniger könnte die H1 somit für das Wirken der UV erklärungskräftig sein. Konkret könnte hier die Beziehung zwischen IT-Unternehmen und der Regierung allgemein indirekter/schwächer ausfallen, vorausgesetzt, Letztere hat Erstere durch Kontroll- und Regulationsmaßnahmen noch nicht stark genug von sich abhängig gemacht. Gleichzeitig verdeutlicht die Episode um Chris Krebs, dass besonders in Demokratien nichtstaatliche AkteurInnen sich in gewisser Weise auch mit der ihnen angedachten Proxy-Rolle identifizieren müssen bzw. eine hinreichende Interessenskonvergenz vorhanden sein muss, damit aus Sicht des staatlichen Sponsors von einer erfolgreichen Staat-Proxy-Beziehung gesprochen werden kann. Dies scheint in Israel bislang noch stärker der Fall zu sein. Im Gegensatz zu Autokratien, in denen persönliche Karrieren noch deutlich stärker von der Loyalität gegenüber dem Regime abhängig sind, führt eine Abstrafung von AkteurInnen wie Chris Krebs in (noch hinreichend libe-

ralen) Demokratien jedoch zu Reputationsverlusten aufseiten der verantwortlichen PolitikerInnen.

Bezüglich der Wirkweise der IV sind aufseiten der USA folgende Befunde relevant: Für die Amtszeiten George W. Bushs können keine Aussagen getroffen werden, da hier auch keine Indizien für die konzeptualisierte Staat-Proxy-Beziehung gefunden wurden. Lediglich die zwei beschriebenen Fälle Agent.BTZ und Operation Mermaid indizieren, dass bereits vor dem Bekanntwerden von Stuxnet autokratische Staaten wie Russland und der Iran den Angriffsvektor der USA im Cyberspace im Kontext gewaltsamer Auseinandersetzungen im Nahen Osten punktuell ausnutzten. Für die Amtszeiten Obamas lassen sich für die H1 aufseiten der IV nur bedingt Evidenzen finden:[158] Lediglich in drei Fällen mit US-Zielen, in denen zwischen 2009 und 2016 IT-Unternehmen eine ›True Attribution‹ vornahmen, wurde ein gewaltsamer HIIK-Konflikt mit zumindest seitens der Cyberangreifer unterstellter US-Beteiligung kodiert. Die übrigen vierzehn Fälle ohne US-Ziele, in denen US-IT-Unternehmen eine ›True Attribution‹ unternommen haben und in denen eine gewaltsame Dimension kodiert wurde, könnten darauf hindeuten, dass die H1 der IV für Demokratien wenn, dann vor allem wörtlich verstanden werden sollte: So könnten die US-IT-Unternehmen nicht nur dem jeweils angegriffenen Land einen Dienst durch ihre Attribution erweisen, sondern auch ihrer eigenen Regierung. Dies erscheint plausibel, wenn der Annahme gefolgt wird, dass die USA unter Obama allgemein an ›Naming-and-Shaming‹-Prozessen gegen Autokratien sowie Resilienzaufbau gegen deren Angriffe interessiert waren und eben nicht nur in Fällen mit US-Opfern. Die für die USA unter Trump eingeschränkte Erklärungskraft der H1 der UV überträgt sich auch auf die H1 der IV für seine Amtszeit, da für beide entscheidend ist, dass die demokratische Cyberproxy-Nutzung nur eingeschränkt festgestellt werden konnte, auch in Fällen mit besonders asymmetrischen Verwundbarkeiten im Cyberspace.

Die H2 der IV kann für die USA insbesondere durch den Wechsel von Obama zu Trump plausibilisiert werden, genauer gesagt den Fall der APT1-Attribution durch Mandiant, jedoch in umgekehrter Lesart:[159] So hatten vor der Veröffentlichung des Berichtes 2013 noch keine signifikanten Sanktionsmöglichkeiten seitens der USA gegenüber China auf der konventionellen Ebene im Raum gestanden. Diese wurden erst danach initiiert, angedroht und in Teilen auch durchgeführt. Somit fällt die Proxy-Attribution nicht in die Kategorie der substituierenden Verantwortungszuweisung, sondern ebnete den konventionellen Sanktionsmaßnahmen erst den Weg. Stattdessen lassen sich die zahlreichen Anklagen während der Amtszeit von Donald Trump sowie die (alleinstehenden) Attributionen von US-IT-Unternehmen stärker in diese Kategorie einordnen. Auch dies lässt sich durch die bereits zu Beginn der Präsidentschaft Trumps umfangreich eingeleiteten Sanktions- und -Konfliktmaßnahmen gegen China erklären, die das allgemeine

158 *H1 (IV): Je stärker die asymmetrische »Cyber«-Verwundbarkeit demokratischer Staaten im Rahmen gewaltsamer konventioneller Konflikte seitens Autokratien manipuliert/ausgenutzt wird, desto wahrscheinlicher ist eine demokratische Cyberproxy-Nutzung.*

159 *H2 (IV): Je stärker eine demokratische Regierung bereits auf der konventionellen Ebene Sanktionsmöglichkeiten gegenüber einem autokratischen Cyberangreifer in Stellung gebracht oder angewandt hat, desto wahrscheinlicher ist eine lediglich substituierende Proxy-Attribution.*

Eskalationsniveau bereits entsprechend erhöht hatten.[160] Trump sah die USA zwar verwundbar gegenüber chinesischen Spionageoperationen, scheute jedoch im Gegensatz zu Obama weniger eine vergleichbare konventionelle Eskalation, was sich durch seine konfliktive Präferenzkonstellation gegenüber China erklären lässt. Hinzu kommt, dass sich Anklagen gegen ausländische HackerInnen zu diesem Zeitpunkt bereits stärker als eine Art ›liberale Ersatzhandlung‹ gegen Individuen, nicht aber deren auftraggebende Staaten selbst etabliert hatten. Staaten waren darüber hinaus infolge der angesprochenen Welle an ›Joint Attributions‹ eher bereit, Attributionsevidenzen untereinander zu teilen.[161] Proxy-Attributionen gegenüber China, die der eigenen Verantwortungszuweisung legitimatorisch den Weg ebnen sollten, erschienen aus dieser Sicht somit weniger notwendig und sollten ab 2017 stärker als eine Art Nebenprodukt der zu dieser Zeit herrschenden Konfliktsituation zwischen den beiden Ländern, auf beiden Konfliktebenen, betrachtet werden. Für US-IT-Unternehmen stellt China nicht nur aufgrund der Operationen gegen US-Ziele, sondern auch aufgrund des weltweiten Spionageradius chinesischer APTs *immer* einen wichtigen ›Threat-Actor‹ dar, da amerikanische Unternehmen über internationalen Marktzugang verfügen.[162]

Die offensichtlich eingeschränkte Erklärungskraft der H1 der IV muss für Israel treffenderweise ambivalent bewertet werden, während die H2 auch hier eher gestützt werden konnte: Eine steigende Ausnutzung von Verwundbarkeiten im Cyberspace im Rahmen gewaltsamer konventioneller Konflikte führte bei Israel gegenüber dem Iran sowie dem Konflikt im Gaza-Streifen zwar zu einer partiellen Aufgabe der ansonsten herrschenden Detektions- und Attributionszurückhaltung durch Quasi-Attributionen, andererseits fokussierten sich, wie dargestellt, viele der Attributionen israelischer IT-Unternehmen auf diese beiden Kontrahenten. Für die H1 der IV wird für Israel somit geschlussfolgert, dass sich die stellvertretenden Proxyattributionen besonders auch auf

160 Monika Kaminska argumentiert für öffentliche Anklagen ähnlich wie die vorliegende Arbeit für Attributionen durch IT-Unternehmen, dass diese zum einen ein Mittel für Staaten seien, ihrer eigenen Attribution ein größeres Maß an Glaubwürdigkeit zu verleihen sowie potenzielle Fehlschlüsse zu vermeiden, da für diese ein höheres Maß an Beweislast erforderlich ist als für Presseerklärungen. Zum anderen seien Anklagen jedoch auch ein Mittel, um noch schwerwiegendere, eskalativere Reaktionsformen zu vermeiden und der Öffentlichkeit zu demonstrieren, dass etwas ›getan werde‹ (Kaminska 2021, S. 8). Auch dies ist eine argumentative Parallele zu den konzeptualisierten Proxy-Attributionen privater IT-Unternehmen.

161 Diese eher ad hoc gebildeten Attributionskoalitionen blieben jedoch in ihrer Zusammensetzung und auch hinsichtlich der Art und des Umfangs der öffentlich gemachten Evidenzen variant. Im Gegensatz zu internen Joint Attributions unterschiedlicher US-Institutionen könnten transnationale Zusammenschlüsse, etwa mit der EU und weiteren gleichgesinnten Demokratien, die konkrete Anwendung geltenden Völkerrechts stärken. Wie für die EU jedoch gezeigt wurde, die bis heute auch keinen offiziell gemeinsamen Attributionsmechanismus etabliert hat, stehen nationale Partikularinteressen einer gemeinsameren und kohärenteren Attribution intern, aber auch auf transatlantischer Ebene bislang oft im Wege (Soesanto 2021). So sehen unterschiedliche EU-Staaten nicht immer dieselben Anreize, ihre Attributionsevidenzen untereinander zu teilen, was jedoch auch aufgrund unterschiedlicher technischer Fähigkeiten für eine stärker europäisierte Sanktionspolitik notwendig wäre. Es muss sich somit noch zeigen, ob die im Falle des Viasat-Hacks plötzlich sehr viel direktere und gemeinsamere Sprache der Erklärung des Rats der EU zur russischen Verantwortlichkeit auch außerhalb des Ukraine-Kontext fortgeführt wird.

162 Gleiches gilt auch für Israel.

GegnerInnen in bewaffneten Konflikten richten, in Einzelfällen jedoch auch ein öffentliches, politisches Signaling erfolgte. Bezüglich der H2 ist besonders die 2019 erfolgte Militärreaktion auf die Cyberzentrale der Hamas von Bedeutung: So war dieser der erste Raketenbeschuss aus dem Gaza-Streifen seit 2014 vorausgegangen. Dies indiziert, dass für die israelische Attributionspolitik besonders die jeweilige konventionelle Konflikt-Situation eine Rolle spielt und, falls notwendig, gewaltsame Eskalationen auch durch politische Quasi-Attributionen und nicht nur technische Proxy-Attributionen gerechtfertigt werden und somit in solchen Fällen tatsächlich nur noch substituierender Natur sind.

6. Befunde und Implikationen

Insgesamt kann für beide Regimetypen konstatiert werden, dass diese aufgrund der aufgezeigten Funktionen ihre Proxys im Cyberspace entgegen der für traditionelle Proxys getätigten Beobachtung stärker als politisches Medium denn als militärisches ansehen (vgl. Moghadam und Wyss 2020, S. 121). Zweitens erscheinen nichtstaatliche AkteurInnen im Cyberspace immer nur so stark, wie es der jeweilige Staat zulässt. Dies gilt für Autokratien, zunehmend aber auch für Demokratien (Stichworte: ›Balkanisierung/Renationalisierung des Internets‹). Nachfolgend werden die zentralen Befunde für beide Regimetypen zusammengefasst und kritisch reflektiert.

6.1 Autokratien und ihre Cyberproxys

Für autokratische Regime und ihre Cyberproxys werden aufgrund der vergleichenden Fallstudien folgende Befunde nochmals betont und kritisch reflektiert:

Ohne völkerrechtlich verbindliche Regeln im Cyberspace, die besonders auch durch Normbildungsprozesse entstehen können, ist der autokratischen Nutzung von Cyberproxys kaum Einhalt zu gebieten. Öffentliche Attributionen demokratischer Länder, die jedoch nicht mit entsprechenden völkerrechtlichen Gegenmaßnahmen kombiniert wurden, entwickelten bislang keine entscheidende Abschreckungswirkung, da Autokratien darauf in erster Linie nicht durch eine funktionale, sondern personelle/organisatorische Umstrukturierung, auch mithilfe von Proxys, reagierten.

Die autokratischen Fallstudien zeigten ferner, dass es scheinbar zu einer Art Proliferation von Strategien, Techniken und Methoden im Cyberspace zwischen autokratischen Staaten kommen kann. Es kann dabei von einer inversen Logik zwischen China und Russland gesprochen werden: Während sich China im Bereich seines offensiven Cyberkonfliktaustrages teilweise inhaltlich durch stärker disruptive und militärisch integrierte Cyberattacken sowie operativ durch die vermehrte Integration unterschiedlicher Proxys wie Unternehmen oder wissenschaftlicher Einrichtungen dem russischen Modell anzupassen scheint, ist für Russland im Bereich der Internet-Governance eine zunehmende Annäherung an das chinesische System der ›Great Firewall of China‹ festzustellen. China übernimmt somit im Cyberkonfliktaustrag gegenüber der externen Umwelt

partiell russische Methoden und Strategien und Russland im Gegenzug chinesische im eigenen Umgang mit der nationalen Informationssouveränität, die nicht zuletzt auch der Abschottung nach außen dienen soll (vgl. Saalman 2017).

In der Analyse wurde zudem gezeigt, dass offensive Proxy-Nutzung tatsächlich auf die jeweilige Interessenlage der autokratischen Führung ausgerichtet ist: So lässt sich z.B. für Russland (zumindest vor dem Angriff auf die Ukraine im Februar 2022 und den daraus resultierten Wirtschaftssanktionen) kein weitflächiger, ökonomisch motivierter Datendiebstahl wie im Falle Chinas beobachten, obwohl dieselbe Praxis ja auch russischen Cyberproxys offen steht. Zentral sind demnach die eigenen Verwundbarkeitsasymmetrien. Dem bloßen Ausnutzen von Gelegenheiten ist geringere Bedeutung beizumessen. Ferner zeigt sich, dass sich Russland mit seinen disruptiveren Cyberoperationen stärker in direkte Opposition zur internationalen, liberal-demokratisch geprägten Staatenumwelt begeben hat, als China. Für die Interessensdurchsetzung der VR galt es auf außenpolitischer Ebene bislang IOs nicht öffentlich zu unterminieren, sondern stattdessen von innen heraus zum eigenen Vorteil zu nutzen, dasselbe gilt für wirtschaftliche Interdependenzverhältnisse mit demokratischen Staaten.

Für den Einfluss der KV auf die autokratische Cyberproxy-Nutzung konnte aufgezeigt werden, dass die Cyberkonflikt-Akteurslandschaft in beiden Fällen die Auswahl der Akteurstypen als Proxys grundlegend bestimmte. Bei Russland waren dies aufgrund des Zerfalls der UdSSR und vieler arbeitsloser InformatikerInnen eher AkteurInnen der Cyberkriminalitätsszene; bei China aufgrund des eingeschlagenen Modernisierungs- und Wirtschaftsentwicklungswegs vor allem auch Frontunternehmen des Technologiesektors. Für China deutet sich durch die zunehmend berichteten Moonlighting-Aktivitäten jedoch ein potenzieller Wandel zu stärkerer Cyberkriminalität von AkteurInnen an, die als staatliche Proxys begonnen haben.

Für Russland ist in der Retrospektive besonders seit Februar 2022 aufgrund des Angriffs auf die Ukraine für den Einfluss des allgemeinen Konfliktniveaus von Interesse, welche Rolle Cyberoperationen allgemein und Cyberproxys im Speziellen hierbei spiel(t)en.. Wirkliche ›Plausible Deniability‹ der vier genannten Hauptgruppierungen (Fancy Bear/APT28, Cozy Bear/APT29, Sandworm und Turla) scheint kaum noch zu existieren. Ist also beispielsweise nach wie vor Sandworm für die Sabotage kritischer Infrastrukturen verantwortlich, da primär nicht mehr die Verschleierung der Verantwortlichkeit im Vordergrund steht, sondern die (erfolgreiche) Durchführung der Operation an sich? Oder wurden neue AkteurInnen, z.B. Hacktivisten oder Cyberkriminelle gefunden, die wieder größere Ambivalenz bei der Attribution im Sinne ›echter‹ Cyberproxys garantieren? Auch die Reaktion westlicher Demokratien auf russische Cyberoperationen kann hierauf einen großen Einfluss nehmen.

Für China wird dagegen die Weiterentwicklung militärischer Konflikte im asiatischen Raum zeigen, inwiefern sich diese Konflikte verschärfen oder entspannen. Anzunehmen ist jedoch Folgendes: Je eskalativer diese konventionellen Konflikte werden, desto stärker wird die SSF eingesetzt, um Manöver durch Cyberoperationen zu ergänzen. Die berichtete Episode um den Stromausfall in Mumbai 2020 hat bereits angedeutet, dass auch China kritische Infrastrukturen militärischer Kontrahenten zunehmend ins Visier nehmen könnte.

Zuletzt deutete die Debatte um international anerkannte und erfolgreiche IT-Unternehmen als mögliche Cyberproxys autokratischer Staaten an, dass auch deren Verhältnis zum eigenen Staat nicht nur von Vorteilnahme geprägt ist: Die KPC reagierte auf aus ihrer Sicht potenziell regimegefährdende Aktivitäten ihrer großen Technologie-Unternehmen wie Alibaba von Jack Ma mit internen Repressionen und auch Russland verschärfte im Umgang mit dem bekannten IT-Unternehmen IB-Group 2021 die staatliche Kontrolle.

6.2 Demokratien und ihre Cyberproxys

Für demokratische Cyberproxys muss konstatiert werden, dass IT-Firmen eher punktuell als wirkliche Proxys im Sinne stellvertretender, durch den Staat beauftragte oder unterstützte Attributionen agieren. Es konnte keine verstetigte Staat-Proxy-Beziehung plausibilisiert werden, wie sie für zahlreiche offensive Proxys autokratischer Regime nachgewiesen werden konnte. Dabei verhinderten wohl auch erwartete wirtschaftliche Einbußen, wenn eine Firma zu sehr als verlängerter Arm der Regierung im Ausland gilt, eine stärkere Proxy-Funktionserfüllung. Verstärkt wird dies durch die steigende technologische Souveränität von Staaten mit wichtigen Absatzmärkten wie z.B. China.

Gleichzeitig verfügen private Unternehmen in Demokratien über eine größere Autonomie gegenüber ihren Regierungen als in den meisten Autokratien, da oftmals marktwirtschaftliche Strukturen dominieren und der Staat somit (zumindest relativ gesehen) weniger Einfluss- und Kontrollmöglichkeiten hat. ›Support‹ des Staates bezieht sich somit zumeist auf allgemeine Unterstützung der Unternehmen durch entsprechende (fehlende) Regulationen oder staatliche Aufträge und weniger auf konkrete Attributionsdirektiven. Der DNC-Hack/Leak demonstriert zudem, dass die Funktion der Schaffung von Legitimation einer erst verspätet erfolgenden politischen Attribution auch dahingehend kontestiert werden kann, falls ein Akteur des politischen Spektrums, in diesem Fall der gewählte Präsident, die Legitimation des (temporär) stellvertretend attribuierenden Unternehmens diskreditiert. IT-Unternehmen können in Demokratien Regierungen und deren Handlungen also nur Legitimation verleihen, sofern deren eigene Legitimation nicht durch Dritte angefochten wird. Die Episode zeigt zudem einmal mehr, dass Attribution schon lange keine rein rechtliche ›Ja/Nein‹-Frage mehr ist, sondern zahlreiche Grautöne, besonders durch Politisierung und Polarisierung, aufweist. Der Aspekt der ›richtigen‹ Vermittlung unterschiedlicher Attributionsevidenzen wird somit für liberale Demokratien immer entscheidender, sofern sie den Konflikt um die Deutungshoheit im Rahmen von Cyberkonflikten nicht an desinformationsorientierte Parteien verlieren wollen.

Obwohl für die USA und Israel defensive Cyberproxy-Funktionen plausibilisiert werden konnten, deutet deren Varianz hinsichtlich der Ausprägung der AV I auf die Relevanz demokratischer Subtypen hin. So wie die Regimetypen-Unterschiede zwischen Russland und China einen erheblichen Teil deren offensiver Cyberproxy-Nutzung erklären konnten (personalistisches vs. Einparteienregime), lassen sich auch die USA und Israel hinsichtlich der republikanischen Ausgestaltung des politischen Systems sowie ideeller und wirtschaftlicher Interessen nicht einfach miteinander vermengen. Vielmehr de-

monstrierten die vergleichenden Fallstudien, dass für die israelische Cyberproxy-Nutzung die Aufrechterhaltung historisch etablierter Taktiken wie der beschriebenen Ambivalenz im Umgang mit sicherheitspolitischen Gefahren eine umfassendere Rolle spielte als für die USA. Deren inhaltliche Cyberproxy-Nutzung hing dagegen stärker von den dominanten Interessensgruppierungen in Abhängigkeit von deren Verhältnis zum Präsidenten ab. Für Israel wird somit retrospektiv in der mittlerweile bereits wieder beendeten Post-Netanjahu-Ära von Interesse sein, inwiefern diese zeitweilige Varianz auf der republikanischen Ebene durch das (vorläufige) Ende der Likud-Ära auch eine Varianz in der Cyberproxy-Nutzung sowie der Cyberkonfliktstrategie im Allgemeinen bewirkt hat.

Sowohl für die USA als auch für Israel gilt es zudem, die seitens verschiedener BeobachterInnen hervorgehobene Nutzung privater AkteurInnen zu offensiven Zwecken im Cyberspace nicht aus den Augen zu verlieren, um das offensive Cyberproxy-Konzept nicht von vornherein auf Autokratien zu beschränken. Unabdingbar wäre hierfür jedoch eine weiterführende Differenzierung der unterschiedlichen Motivlagen, Staat-Proxy-Beziehungsmuster sowie rechtlichen Attribute zwischen autokratischen und demokratischen Cyberproxys im Offensivbereich, da hierbei – wie im Rahmen dieser Arbeit konstatiert – deutliche Unterschiede existieren.

Für Demokratien im Allgemeinen ist zudem die Etablierung von ›Plausible Deniability‹ im Cyberspace von Bedeutung: So könnte es entsprechend berichteter Beispiele aus dem konventionellen Bereich auch für Operationen im Cyberspace der Fall sein, dass sich demokratische Regierungen gegenüber geheimen Operationen ihrer SicherheitsakteurInnen in gewisser Weise absichern, um bei deren ungewollter Veröffentlichung eine Kenntnisnahme derselbigen ›plausibel bestreiten‹ zu können (vgl. Knott 2014). Da eine solche Praxis jedoch die Kontrolle der Politik über staatliche Behörden potenziell schwächen kann, gilt es, die Berichtspflichten demokratischer Cybereinheiten im Rahmen ihrer Offensivbefugnisse im Vergleich zwischen präsidentiellen und parlamentarischen Systemen kritisch auf den Prüfstand zu stellen.

6.3 Theoretische Implikationen

Der Liberalismus hat sich als tragfähiger theoretischer Ansatz erwiesen, um autokratische und demokratische Cyberproxy-Nutzungen zu analysieren. Bedeutsam ist sein Fokus auf nichtstaatliche AkteurInnen und deren Interessen: Nicht nur die reinen Machtasymmetrien entscheiden, wie vom Realismus vorhergesagt, über den Cyberkonfliktaustrag. Ansonsten dürfte es erstens neben den USA und vereinzelten weiteren Staaten keine im Cyberspace (erfolgreich) aktiven Staaten geben; zweitens dürften nichtstaatliche AkteurInnen dabei keine Rolle spielen; drittens dürfte es zwischen demokratischem und autokratischem Cyberkonfliktaustrag aufgrund der inneren Verfasstheit keine Unterschiede geben, zwei ähnlich ›mächtige‹ Demokratien und Autokratien müssten sich auch ähnlich verhalten; viertens müsste die Reaktion demokratischer Staaten auf autokratische Cyberangriffe ähnlich ausfallen wie die Reaktion auf Angriffe demokratischer Staaten, wenn deren Machtpotenziale als ähnlich gefährlich seitens der angegriffenen Demokratie eingeschätzt werden bzw. sonstige Interessenskonvergenzen keine Rolle spielen; und fünftens dürfte es zu keiner (*nicht*

hegemonial-indizierten) Kooperation im Cyberspace kommen. Stuxnet und weitere geheimdienstliche Kooperationen, etwa zwischen dem niederländischen Geheimdienst und dem FBI bei der Attribution von Cozy Bear 2016, beweisen jedoch das Gegenteil, da diese nicht als hegemonial indiziert betrachtet werden.

Dennoch zeigen der HD-CY.CON und dessen durchaus sozialkonstruktivistischer Ansatz gemäß dem Grundsatz »*Attribution is what states make of it*« (Rid und Buchanan 2015, S. 7), dass auch rationalistische Theorien wie der Liberalismus in Teilen durch sozialkonstruktivistische Elemente ergänzt werden könnten. So hat die Analyse auf Basis öffentlich zugänglicher Quellen und der darin berichteten Verantwortungszuweisungen entsprechend des liberalen Erklärungsansatzes plausibilisiert, inwiefern dieser die autokratische vs. demokratische Cyberproxy-Nutzung erklären kann. Wie vom Ansatz fokussiert, stellten die jeweiligen Präferenzordnungen der zentralen Interessensgruppen der Staaten die zentrale Erklärungsvariable dar, über die erklärt werden konnte, welche Asymmetrien mit welchen Proxy-Funktionen und durch welche Proxys verändert/manipuliert werden sollten. Die Dreiteilung in ideellen, kommerziellen und republikanischen Liberalismus ermöglichte es, den Einfluss der institutionellen Ausgestaltung des politischen Systems auf den Herrschaftszugang einzelner Gruppen zu identifizieren und in einem zweiten Schritt deren ideelle sowie kommerzielle Interessen zur staatlichen Cyberproxy-Nutzung in Beziehung zu setzen. Da sich die Analyse auf die im HD-CY.CON erfassten Kategorisierungen der einzelnen Gruppen und ihrer Angriffe als staatlich gesponsert bzw. allgemein/direktstaatlich stützte, ist dabei implizit die soziale Konstruktion der Attribution des Angreifers seitens der jeweiligen Attributionsquelle mit angelegt. Diesem Umstand wurde jedoch insofern Rechnung getragen, als im empirischen Teil entsprechend des Spektrums staatlicher Verantwortlichkeit untersucht wurde, inwiefern sich die jeweiligen Attributionen auf Basis öffentlicher Informationen stützen oder entkräften lassen. Dies verdeutlicht, dass auch das Cyberproxy-Konzept wie das Proxy-Konzept im Allgemeinen nicht frei von Deutungskonflikten ist.

Ferner entscheidet das normative Framing der eigenen Cyberproxy-Nutzung sowie der Fremdwahrnehmung besonders aufseiten befreundeter/alliierter Staaten über den öffentlichen Umgang hiermit, bzw., ob diese ebenso wie autokratische Cyberproxy-Spionage als unrechtmäßiges Verhalten angesehen bzw. öffentlich als solches deklariert wird. So waren und sind die USA offensichtlich davon überzeugt, dass ihre technologische Vormachtstellung dem Wohle der westlichen Staatenwelt dient und sie verpflichtet sind, alle möglichen Ressourcen zur Prävention oder Präemption potenziell staatsgefährdender Kräfte zu nutzen. Neben dem Liberalismus könnte also auch die sozialkonstruktivistische Rollentheorie ein geeigneter Ansatz zur Erfassung von Cyberproxys sein. Als Einschränkung wird hier jedoch eingewandt, dass das Proxy-Konzept stärker eine theoretische Meta-Rolle darstellt, die von außen AkteurInnen zugesprochen wird. Für eine rollentheoretische Analyse sollte die Proxy-Rolle somit mit weiteren, inhaltlichen Rollenkonzeptionen verbunden werden. Ansonsten ließen sich Bezüge zum Ego-Teil der jeweiligen Proxyrollenkonzeption wahrscheinlich weitaus schwerer herstellen als zum Alter-Teil.

In jedem Falle verschwimmt in der Empirie die Trennlinie zwischen tatsächlichen Proxys und direktstaatlichen Angriffen immer mehr, was gleichzeitig die beschriebenen theoretischen Herausforderungen und definitorischen Unterschiede in der Cyberproxy-

Konzeptualisierung erklärt. Angesichts der steigenden allgemeinen bzw. direktstaatlichen Attributionen demokratischer Staaten gegen autokratische CyberangreiferInnen stellt sich die Frage nach dem ›Verfallsdatum‹ des (offensiven) Cyberproxy-Konzepts. Wird die autokratische ›Plausible Deniability‹ immer unplausibler, könnten autokratische Regime wie Russland oder China, die auch auf staatlicher Ebene die notwendigen Fähigkeiten zur Durchführung von Cyberoperationen besitzen, in Zukunft auf Proxys ganz verzichten. An dieser Stelle gilt es jedoch zwischen der Proxy-Attribution und der tatsächlichen Einsetzung zu unterscheiden: Da neben der ›Plausible Deniability‹, wie aufgezeigt, auch interne Coup-Proofing-Erwägungen sowie fehlende Eigenkapazitäten auf autokratischer Seite zur Einsetzung von Proxys führen können, hätte eine gewandelte demokratische Attributionspraxis auf diese beiden stärker domestisch geprägten Motivlagen deutlich weniger Einfluss. In jedem Falle wird die Frage der rechtlichen Verantwortung der Staaten immer stärker Gegenstand politischer und daher notwendigerweise auch wissenschaftlicher Debatten.[1]

Es könnte somit in Zukunft zu einer Art Normalisierung offener direktstaatlicher Cyberangriffe kommen, wobei interessant sein wird, speziell die israelische Kommunikationsstrategie bezüglich eigener Operationen im Wandel der Zeit zu betrachten. Jedoch bleibt hierbei abzuwarten, inwieweit die Intensitätsschwelle, die das jeweilige Opfer zu einer physischen Reaktion zwingen würde, dabei regelmäßig und in welcher Form überschritten wird. Aus theoretischer Sicht stellt sich somit folgende Frage: Treibt die tatsächliche Staatenpraxis die internationale Normgenese vor sich her oder umgekehrt?

Ein weiterer theoretisch-analytischer Mehrwert der Arbeit betrifft den Umgang mit dem Proxy-Konzept an sich: Indem Proxys zum einen im Rahmen von Cyberoperationen untersucht wurden, dabei jedoch (auch) deren Beziehungen zum jeweiligen staatlichen Sponsor im Mittelpunkt standen sowie ferner Bezüge zu damit assoziierten konventionellen Konflikten hergestellt wurden, wurden in der Arbeit die beiden in der Proxy-Forschung bislang dominierenden Ansätze verbunden: der akteurszentrierte vs. der konfliktdomänenzentrierte Ansatz (Moghadam und Wyss 2020, S. 124). Hierdurch wird deutlich, dass nichtstaatliche AkteurInnen als Proxys im Cyberspace dienen können, dies jedoch zeitlich begrenzt sowie auf verschiedene Konfliktsphären bezogen sein kann. Cyberproxys stellen eben zumeist *nicht* das alleinige Konfliktmittel autokratischer und demokratischer Staaten dar, sondern eines unter mehreren. Die Übertragung des bislang rein offensiv verwendeten Cyberproxy-Konzepts auf demokratische Attributionspraktiken soll aufzeigen, welchen Nutzen das Proxy-Konzept zur theoriegeleiteten Erfassung demokratischer Verschleierungs- und Geheimhaltungstaktiken im Rahmen von Cyberkonflikten haben kann. Dennoch sollte bei einer solchen Modifikation eines bestehenden Konzepts stets die Gefahr eines »*concept stretching*« (Sartori 1970, S. 1034) berücksichtigt werden: Das Ziel sollte nicht sein, möglichst viel Empirie durch dasselbe Theoriekonzept erfassen zu können, sondern durch die Rekontextualisierung des Konzepts dessen Anknüpfungsfähigkeit auch an neuere Untersuchungsfelder zu überprüfen und ggf. auch

1 So beschäftigte sich im Jahr 2022 die ›Closing the Gap‹-Konferenzreihe des ›The Hague Program on International Cyber Security‹, gemeinsam u.a. mit der Initiative ›EU Cyber Direct‹, mit dem Thema der »*Responsibility in Cyberspace*« (s. The Hague Program on International Cyber Security 2022).

kritisch zu hinterfragen. Im Falle der hier konzeptualisierten demokratischen Cyberproxy-Nutzung ist sicherlich am stärksten der Delegations-/Unterstützungsmodus seitens Demokratien an IT-Unternehmen im Rahmen des Attributionsprozesses zu diskutieren. Es stellt sich konkret die Frage, wie direkt und fallspezifisch dieser (nachweisbar) sein sollte, um das Proxykonzept zur Anwendung bringen zu können.

Die empirischen Befunde zur Untersuchung russisch- und chinesischsprachiger Quellen legen ferner nahe, dass die Cyberkonfliktforschung ihren westlichen Bias auch nicht durch die Inklusion einzelner nichtwestlicher Quellen verliert. Erstens ist an diese nach wie vor schwerer heranzukommen, zweitens weisen diese ebenfalls Verzerrungen auf und drittens dominieren die westliche Sicht und die englische Sprache den Diskurs in der Threat Intelligence Community, insbesondere durch eine nach wie vor auf vielen Ebenen bestehende US-Dominanz. So sind die meisten verwendeten Komponenten der globalen IT-Infrastruktur wie Kabel, Software-Produkte, Hardware-Produkte, Social-Media-Plattformen etc. US-Produkte, wodurch sich auch der Streit um die Involvierung Huaweis am Aufbau der 5-G-Netze erklärt.

6.4 Anknüpfungspunkte für künftige Forschungsvorhaben

Aus den diskutierten empirischen Befunden und theoretischen Überlegungen ergeben sich zahlreiche Anknüpfungspunkte für künftige Forschungsvorhaben im hier bearbeiteten Themenfeld.

Beginnend mit der VR China als Untersuchungsfall, könnten weitere Studien analysieren, inwiefern Xis personalisierter Machtzugang in Zukunft stärker durch KPC-Eliten kontestiert wird und welchen Einfluss dies auf den offensiven Cyberkonfliktaustrag des Landes hat. Zudem stellt sich die Frage, wie die PLA im Falle einer Eskalation im Südchinesischen Meer oder gegen Taiwan im Cyberspace performieren würde. Konkret könnte dabei die Rolle von Cyberoperationen auf strategischer, operativer und taktischer Ebene untersucht werden.

Daran anknüpfend könnte jedoch auch die Rolle der PLA auf domestischer Ebene Gegenstand weiterer Arbeiten sein, etwa um herauszufinden, ob sie auch disruptiv gegen nationale Ziele vorgeht und, falls ja, in welchem Zusammenhang dies mit gewaltsamen Repressalien gegen die betroffenen AkteurInnen steht.

Für das MSS wird die Zukunft zeigen müssen, ob es an der in dieser Arbeit aufgezeigten Nutzung kommerzieller Proxys auch in Zukunft festhält. Künftige Arbeiten könnten somit den Einfluss der KV über die Zeit in den Blick nehmen: Ist in Zukunft für China eine noch stärkere Nutzung von Moonlightern bzw. Cyberkriminellen zu erwarten? Falls ja, welchen Einfluss nahmen demokratische Sanktionen (auch im Rahmen der Cyber Diplomacy Toolbox der EU) gegenüber den bislang als Proxys präferierten Frontunternehmen hierauf? Schiebt das MSS in Zukunft den kriminellen Aktivitäten der Moonlighter einen Riegel vor aufgrund steigenden internationalen Drucks und im Vergleich zu Russland salienterer, wirtschaftlicher Interdependenzbeziehungen zu demokratischen Staaten? Welche Rolle könnte dabei analog zur russischen ›Ransomware Diplomacy‹ in der Ukraine-Krise eine mögliche Zuspitzung des Konflikts um Taiwan spielen und den chi-

nesischen Umgang mit nationalen HackerInnen als Verhandlungsmittel gegenüber dem Westen?

Auch für Chinas Verhalten auf internationaler Ebene ergeben sich weiterführende Fragen: Wird die VR auch im Rahmen internationaler Verhandlungen über die Verregelung des Cyberspace eine noch proaktivere Rolle einnehmen, ähnlich wie Russland im Bereich der Cyberkriminalität? Falls ja, inwiefern sind die dabei artikulierten Interessen/Forderungen am eigenen Cyberkonfliktaustrag ausgerichtet bzw. inwiefern soll dieser hierdurch geschützt bzw. ermöglicht werden?

Für Russland bleibt auch nach dieser Arbeit weitgehend unklar, inwiefern Proxys oder Hacker unterschiedlicher Geheimdienste die Operationen der anderen versuchen zu kompromittieren, um deren Interessensdurchsetzungschancen zu schwächen oder einzuhegen. Indizien für ein solches Verhalten gibt es auf der konventionellen Ebene bereits. Die noch tiefergehende Analyse des Verhältnisses der verschiedenen russischen Cyberoperationen im Hinblick auf die grundlegende und jeweils temporäre Beziehung der im Hintergrund verantwortlichen Teile der Winning Coalition zueinander könnte somit einen weiteren Beitrag der Forschung zum russischen Cyberkonfliktaustrag darstellen und auf den Erkenntnissen dieser Fallstudie aufbauen. Dies gilt insbesondere für den Zeitraum während (und potenziell nach) dem Krieg gegen die Ukraine ab Februar 2022, der zu Verschiebungen innerhalb des russischen Machtgefüges auf der konventionellen sowie der Cyber-Ebene führen dürfte.

Weitere Arbeiten könnten für Russland zudem das Verhältnis von Ransomware-Gruppierungen zu staatlichen Stellen sowie deren Integration in die russische Kriegsstrategie in der Ukraine in den Blick nehmen. Die sogenannten »Conti-Leaks« haben gezeigt, dass ursprünglich ökonomisch motivierte Akteure im Kontext geopolitischer Konflikte ihre Präferenzordnung zu Gunsten ideell-nationaler Interessen verändern können und somit nicht mehr als Cyberproxys agieren wollen.[2] Interne Interessenskonflikte können somit die Nützlichkeit einzelner Proxygruppierungen über Zeit schwächen und alternative Rekrutierungsaktionen, wie etwa die Mobilisierung von Gefängnisinsassen mit IT-Kenntnissen in Russland erforderlich machen (Krebs 2022). Nichtsdestotrotz kann Ransomware für Russland (wie bereits zuvor für Nordkorea) ein Baustein sein, um zumindest zeitweise den Druck internationaler Sanktionen abzumildern und so die eigene, Output-orientierte Regimesicherheit durch die erbeuteten Gewinne zu stärken.

Für die Zeit nach Putin wird von besonderem Interesse sein, inwiefern dessen Nachfolger gleichsam im Stande sein wird, das Konkurrenzstreben der Geheimdienste in weitgehend geordneten Bahnen zu halten, oder ob sich einzelne Teile daraus zu einer ernsthafteren Bedrohung für den Kreml entwickeln, als es unter der personalisierten und zentralisierten Führung Putins bislang der Fall war. Die Interessensdurchsetzung der verschiedenen Geheimdienste unter Putin scheint dagegen weniger von deren Bedrohungspotenzial als ihrer faktischen Performanz zur Regimesicherung abhängig zu sein. Ein Machtverlust der Kreml-Spitze nach Putin gegenüber Teilen der Winning

2 Ein mutmaßlich ukrainisches Mitglied der Ransomware-Gang Conti hatte nach deren öffentlicher Loyalitätsbekundung zu Russland interne Daten und Informationen u.a. auch Source-Code der Gruppe öffentlich gemacht (Knop 2022).

Coalition könnte auch einen Einfluss auf das hier analysierte russische Cyberkonfliktverhalten haben, zu größeren Kollateralschäden, noch häufiger sich konterkarierenden Paralleloperationen sowie noch stärkeren geopolitischen Verwerfungen führen. Ein ›Post-Putin‹-Russland könnte jedoch auch stärker demokratische Züge annehmen, je nachdem, wie stark der Modus des Machtübergangs seitens des Regimes gesteuert wird. Käme es aufgrund von zunehmenden domestischen Protesten, etwa aufgrund des (Ausgangs des) Kriegs gegen die Ukraine zu Wahlen, in denen liberale Oppositionsparteien eine tatsächliche Chance auf die Mehrheit hätten, könnte sich auch der russische Cyberkonfliktaustrag in Zukunft ›liberalisieren‹, demnach weniger die Unterwanderung liberal-demokratischer Länder sowie Institutionen zum Ziel haben. Ein solches Szenario erscheint zum aktuellen Zeitpunkt jedoch unwahrscheinlich.

China und Russland sind jedoch nicht die einzigen untersuchungswürdigen Autokratien im Cyberspace. Neben dem Iran und Nordkorea verweisen IT-Unternehmen auch immer wieder auf Vietnam und dessen Cybergruppierungen. Das US-Unternehmen Meta (vormals Facebook) veröffentlichte Ende 2020 einen Bericht, in dem Cyberoperationen mit vietnamesischen Technologie-Unternehmen in Verbindung gebracht wurden (Gleicher 2020). Somit könnte eine potenziell autokratische Cyberproxy-Strategie-Diffusion in den Blick genommen werden bzw. untersucht werden, ob es so etwas wie autokratische Staat-Proxy-Beziehungszyklen gibt, anhand derer prognostiziert werden kann, zu welchem Zeitpunkt ein Land primär auf welche nichtstaatlichen AkteurInnen als Cyberproxys zurückgreifen wird. Regionale Gemeinsamkeiten sowie Subtypenkategorisierungen könnten hierfür theoretische Ansatzpunkte sein.

Da in der vorliegenden Arbeit die Kategorisierungen ›Free‹ vs. ›Not Free‹ von Freedom House verwendet wurden, um möglichst große Regimetypenunterschiede zwischen den Fällen zu gewährleisten, wären für die Zukunft Studien zu hybriden oder im Transformationsprozess befindlichen Staaten wichtig (›Partly Free‹). Da im HD-CY.CON nur neun Proxy- und zehn allgemeine/direktstaatliche Operationen diesen Regimen als AngreiferInnen zugesprochen wurden, deutet sich bei diesen ein im Vergleich zu Autokratien und Demokratien deutlich niedrigeres Cyberoperationsengagement an. Künftige Forschungen könnten sich somit speziell mit diesen Regimen befassen und untersuchen, wie sich deren Cyberoperationsverhalten bei einer autokratischen oder demokratischen Transition verändert. Als theoretischer Anknüpfungspunkt könnte hier die Debatte um unterschiedlich hohe ›Eintrittsschwellen‹ in den staatlichen Cyberkonfliktaustrag dienen, die Max Smeets in seinem 2022 veröffentlichten Buch diskutiert.

Wie bereits angesprochen, stellt sich für Demokratien auch in Zukunft die Frage, ob im Cyberspace die tatsächliche Staatenpraxis die Normentwicklung vor sich hertreibt oder umgekehrt. In diesem Zusammenhang könnte der Einfluss unilateral gesetzter Cybersicherheitsstrategien (z.B. von Großbritannien Ende 2021) auf den demokratischen Normdiskurs und die Normgenese der internationalen Ebene untersuchungswürdig sein. Unmittelbar hiermit verbunden ist die nach wie vor nicht ausreichend behandelte Frage nach der Effektivität bisheriger und künftiger demokratischer Reaktionsoptionen auf autokratische Cyberoperationen. Konkret betrifft dies die EU Cyber Diplomacy Toolbox, die der EU mehr Schlagkraft bei der Bekämpfung und Abschreckung künftiger Angriffe verleihen soll. Daher sollte die bislang noch mehr auf den Aspekt der Attri-

bution ausgerichtete wissenschaftliche Debatte hieran noch stärker anknüpfen bzw. nachgelagerte Aspekte der Verantwortungszuweisung deutlicher berücksichtigen.

Für die USA wird ähnlich wie bei Regierungswechseln in Russland, China sowie Israel von Interesse sein, welchen Einfluss eine mögliche Wiederwahl Donald Trumps (oder ein republikanischer Sieg im Allgemeinen) 2024 auf die künftige Cyberpolitik des Landes haben könnte. Entscheidend könnte sein, auf welchem Stand die internationale Normgenese zu dieser Zeit wäre und ob sie sich entsprechend robust genug gegenüber potenziellen Unilateralismus- und Protektionismusbestrebungen einer republikanischen US-Regierung zeigen würde.

Für Israel als besonders stark von den eigenen Technologieexporten abhängige Demokratie wird sich infolge der Pegasus-Enthüllungen 2021 zeigen, ob und wie sich der Druck anderer Demokratien auf deren Geschäftsbeziehungen zu autokratischen Staaten auswirkt. Kommt es zu einer kontinuierlichen Präferenz für liberal-demokratische Grundwerte vor kommerziellen Interessen? Welchen Einfluss nimmt dies auf die Beziehung zwischen dem öffentlichen und privaten Sektor und die hier konzeptualisierte demokratische Cyberproxy-Nutzung? Auch hieran könnten künftige Forschungsarbeiten anknüpfen.

Ein letzter Aspekt betrifft die in der Arbeit angestrebte Methode unterstützender ExpertInneninterviews: Trotz zahlreicher und wiederholter Kontaktaufnahmen zu unterschiedlichen Akteursgruppierungen in unterschiedlichen Ländern über bereits bestehende Kontakte sowie offizielle Kanäle waren nur in wenigen Fällen Personen zu Interviews bereit. Dies betraf besonders politische/staatliche Institutionen in Deutschland. MitarbeiterInnen der Behörden meldeten konkret zurück, dass sie entweder generell keine Aussagen zu dieser Thematik äußern dürfen oder in Deutschland das Bundesamt für Verfassungsschutz (BfV) für öffentliche Attributionen zuständig sei. Das BfV erlaubt jedoch nur Interviews mit dem Präsidenten, was im Rahmen dieser Arbeit auch keine realistische Option war. Die Interviews mit den wissenschaftlichen Mitgliedern der US Cyber Solarium Comission deuten eine größere Offenheit der USA zu dieser Thematik an, gleichzeitig handelte es sich bei Brandon Valeriano und Erica Borghard auch um keine politischen EntscheidungsträgerInnen oder offizielle US-BeamtInnen. Eine transparentere Cybersicherheitspolitik demokratischer Staaten könnte für die Zukunft dieses offensichtlich zumindest in Teilen bestehende Vertraulichkeitsproblem gegenüber der Wissenschaft etwas aufbrechen, was den Raum für mehr solcher Interviews öffnen würde, die sich explizit mit öffentlicher vs. technischer Attribution von Cyberoperationen befassen.

6.5 Policy-Implikationen

Die Festlegung und öffentliche Kommunikation gewisser roter Linien erscheint auch für den staatlichen Cyberkonfliktaustrag auf internationaler Ebene unabdingbar. Dies sollte jedoch idealerweise nicht durch das Setzen unilateraler Grundsätze erfolgen, indem jeder Staat für sich selbst im Rahmen seiner nationalen Cybersicherheitsstrategie definiert, in welchen Fällen welche Formen offensiver oder reaktiver Cyberoperationen angewandt werden. Vielmehr sollte der bereits in zahlreichen Foren eingeschlagene Mul-

tistakeholder-Ansatz noch intensiviert werden, wobei jedoch eine effektivere Übertragung der dabei erzielten Ergebnisse auf letztlich ›verbindliche‹ Governance-Formate wie die UN notwendig wäre. Den hierfür notwendigen politischen Konsens herzustellen, ist alles andere als leicht. Begonnen werden sollte aus demokratischer Sicht mit den noch unentschlossenen demokratischen oder zumindest hybriden ›Swing States‹: Diese weisen grundlegende Interessenskonvergenzen mit demokratischen Ländern auch bezüglich des Cyberspace auf, tendieren in konkreten Fragen der Internet-Governance jedoch auch zu autokratischeren Modellen. In Joseph Nyes Worten müssten insgesamt demokratische Soft-Power-Potenziale somit autokratische Hard-Power-Potenziale als Anreizstruktur auch für diese Staaten überwiegen, damit sie sich in Grundsatzfragen auf die Seite des liberal-demokratischen Lagers stellen. Policy-Optionen hierfür wären z.B. substanzielle Unterstützungsleistungen bereits stärker entwickelter Staaten für den Aufbau nationaler Kapazitäten im Technologie-Bereich sowie ›Confidence-Building-Measures‹. Diese Unterstützungsleistungen sollten jedoch an demokratische Bedingungen geknüpft werden, damit die zu entwickelnden Fähigkeiten auch entsprechend eingesetzt werden. Grundvoraussetzung hierfür ist jedoch auch innerhalb der als liberale Demokratien bezeichneten Staatengemeinschaft ein Konsens über die hiermit angestrebten Ziele.

Gleichzeitig darf durch ein Kommunizieren roter Linien autokratischen AngreiferInnen nicht zu leicht signalisiert werden, dass alles unterhalb dieser Schwelle stillschweigend geduldet wird, denn sonst könnte dies konsequent und überbordend ausgenutzt werden. Zwei Wege wären hierfür denkbar: Der erste Weg würde über eine gesteigerte und effektivere Sanktionierung der jeweils als Täter identifizierten Autokratien führen. Hierfür müssten jedoch die den Sanktionen zu Grunde liegenden Attributionen auf breiten Konsens innerhalb der einzelnen Staaten sowie untereinander stoßen, da für deren Effektivität eine breite Anwendung seitens möglichst vieler Staaten notwendig ist. Diese Entscheidungen sollen durch ideelle Überzeugungsarbeit und weniger über das Androhen zwischendemokratischer Sanktionierungen wie das Aufkündigen des gegenseitigen Austauschs geheimdienstlicher Informationen erfolgen. Hierfür wäre jedoch das Erreichen des ›Tipping-Points‹ im ›Norm-Life-Cycle‹ erforderlich, damit es zu solch einer Norminternalisierung kommen kann (vgl. Finnemore und Sikkink 1998). Der zweite Weg sähe vor, dass im Zuge komplexen Lernens entsprechende Normbildungsprozesse entstehen. Dies könnte auf internationaler Ebene durch Issue-Linkage ermöglicht werden. Es stellt sich hierbei die Frage nach dem kollektiv besten Ergebnis und wie dieses durch gegenseitige Zugeständnisse über verschiedene Politikfelder hinweg erreicht werden kann. Wenn beispielsweise Autokratien im Rahmen der UN hinsichtlich eines angestrebten Cyberwaffenvertrages entgegengekommen wird, könnten diese als Gegenleistung verbindlich zusichern, keine Angriffe mehr auf demokratische Wahlen und deren IT-Infrastruktur durchzuführen. Bevor es hier jedoch zu einer wirklichen Norminternalisierung auf autokratischer Seite kommen könnte, würde insbesondere Verifikations- und Sanktionsmechanismen zur Überprüfung der ›Compliance‹ dieses Austauschs an angestrebten Gütern auf internationaler Ebene eine wichtige Bedeutung zukommen. Bereits für diese Verifikationsregime ist jedoch ein hinreichendes Maß an zwischenstaatlicher Kooperation notwendig, gerade in einem von Geheimhaltung geprägten Konfliktmedium wie dem Cyberspace. Daher würde

etwa eine internationale Cyberkonflikt-Attributionsagentur, ähnlich der Internationalen Atomenergie-Organisation (IAEA), noch größeren Herausforderungen in ihrer täglichen Arbeit gegenüberstehen als Regime des konventionellen Bereichs. Bereits für die Etablierung solcher Verifikationsregime, die letztlich Norminternalisierung erst ermöglichen sollen, ist somit ein Grundkonsens bezüglich der dem Regime zugrunde liegenden Normen notwendig (vgl. Haas 1980, S. 358).

Wie sich im Zuge des russischen Krieges gegen die Ukraine ab Februar 2022 zeigte, gilt es aus demokratischer Sicht zudem, die autokratischen Handlungen im Cyberspace im Rahmen gewaltsamer Konflikte nicht zu über- oder unterschätzen (vgl. Lonergan und Lonergan 2022). So sollten Cyberoperationen weder als deterministische Ankündigung nachfolgender Militärhandlungen gewertet noch ignoriert werden. Der Ansatz der USA unter Biden, die Ukraine durch die Entsendung von IT-ExpertInnen direkt bei der Prävention und Abwehr russischer Cyberoperationen zu unterstützen (Cooper und Barnes 2021), erscheint dabei sinnvoll, trägt er doch zu keiner direkten Eskalation des Konfliktes bei und stärkt gleichzeitig die ukrainische Cyberdefensive. Generell kann festgestellt werden, dass im Cyberspace ein defensiver »*deterrence by denial*« -Ansatz weitaus erfolgsversprechender erscheint, als der oftmals propagierte »*deterrence by punishment*«-Ansatz der Offensive (vgl. Nye 2017). Verstärktes Engagement zur Stärkung der Cyberdefensive nationaler sowie internationaler IT-Infrastrukturen, auf staatlicher und privater Ebene, sollte somit das oberste Ziel aller Regierungen sein. Gleichzeitig sollten besonders auf transatlantischer Seite Vorbereitungen für den Fall getroffen werden, dass Russland wie 2015/2016 doch noch (physisch) disruptive Cybersabotageoperationen gegen kritische Infrastrukturen der Ukraine, jedoch auch unterstützender Staaten, durchführen sollte. Um die Ukraine nicht noch stärker zum russischen ›Testbattlefield‹ im Cyberspace werden zu lassen, sollten daher klare Reaktionsoptionen für unterschiedliche russische Cyberoperationen abgesprochen und dann auch angewandt werden. Wie die US-Unterstützung der Ukraine entspräche dies der Umsetzung des UNGGE-Reports aus 2015, der die Gefahren von Cyberoperationen gegen kritische Infrastrukturen als einen Schwerpunkt hatte. Dieselbe Logik gilt auch für Taiwan und andere Länder im Südchinesischen Meer, sollten sich chinesische Cyberoperationen im Rahmen militärischer Auseinandersetzungen in Zukunft intensivieren. Insbesondere die Rolle offensiver Cyberproxys als AngreiferInnen sollte hierbei klar als unzureichend definiert werden, um den jeweils auftraggebenden Staat von einer auch rechtlichen Verantwortung freizusprechen. Individuelle Anklageerhebungen, zudem ohne strafrechtliche Effektivität, erscheinen hier bislang als unzureichende Mittel. Notwendig wären somit umfassende und glaubwürdige Attributionspraktiken auf Grundlage völkerrechtlicher Prinzipien, um sich nicht dem Vorwurf rein politisch motivierter Anschuldigungen auszusetzen. Dieser Punkt schließt an die noch stärker zu vereinheitlichende Attributionspraxis demokratischer Staaten gegenüber autokratischen CyberangreiferInnen an, was bereits bei den sich teilweise widersprechenden Namensgebungen von APTs beginnt. Dass dies in Zukunft auch einen Einfluss auf Schadensersatzforderungen im Rahmen abgeschlossener Versicherungen haben könnte, zeigen die Ausführungen der britischen ›Lloyd's Market Association‹ vom November 2021: Darin werden Cyberoperationen mit staatlicher Urheberschaft als Ausnahmen definiert, in welchen der Versicherungsschutz nicht greifen würde. Als zentraler Indikator hierfür wird die politische Attribution der Regierung des Landes benannt,

indem sich die betroffenen Computersysteme befinden. Findet eine solche politische Attribution jedoch nicht oder nur verzögert statt, könne der Versicherer eine Attribution in Richtung staatlicher AkteurInnen auch selbst vornehmen (Lloyd's Market Association 2021). Somit könnten hier neben privaten IT-Unternehmen weitere nichtstaatliche AkteurInnen künftig Cyberattributionen vornehmen, bislang noch nicht hinreichend definierte Standards weiter aufweichen und zudem aus kommerziellem Interesse auch Attributionsdruck auf nationale Regierungen ausüben.

Ferner sollten verschiedene Attributionsformen auch an unterschiedliche Reaktionsoptionen gekoppelt werden, um hier eine bessere Verhaltenserwartbarkeit zu schaffen (z.B. im Rahmen der EU Cyber Diplomacy Toolbox). Dies sollte aber auch hinreichend flexibel gehandhabt werden, um (wie zuvor angedeutet) zu verhindern, dass eine Autokratie das Verbleiben unter einer als besonders kritisch angesehen Intensitätsschwelle konsequent perfektioniert, die eigenen Operationen immer mehr ausweitet und so zu einer Normalisierung dieser Cyberoperationen beiträgt. Auch für einen solchen Fall sollten im Sinne einer kumulativen Intensitätsbewertung verhältnismäßige Reaktionsoptionen entwickelt werden.

Innerhalb der EU wird seit mehreren Jahren verstärkt das Konzept der ›technologischen/digitalen Souveränität‹ diskutiert, um weniger abhängig von den USA und Asien sowohl im Rahmen internationaler Lieferketten als auch bezüglich des Austausches geheimdienstlicher Informationen im transatlantischen Verhältnis zu werden. Letzteres erschien insbesondere aufgrund der Präsidentschaft Donald Trumps notwendig, der zuvor etablierte Prinzipien der Zusammenarbeit negierte und verstärkte Unsicherheit aufseiten der EuropäerInnen hervorrief. Sowohl aus wirtschaftlicher als auch sicherheitspolitischer Sicht könnte eine verstärkte Autonomie der EU somit positive Effekte haben, etwa indem der Zugang der USA zu Geheimdienstinformationen aus dem EU-Raum an Bedingungen geknüpft würde. Damit sich die EU diese Forderungen jedoch überhaupt leisten kann, wäre der Ausbau eigener geheimdienstlicher Kapazitäten erforderlich. Inwiefern dies bedeuten würde, dass die Geheimdienste der EU-Mitgliedstaaten hierzu vermehrt in fremde Netzwerke eindringen müssten, Sicherheitslücken ausnutzen und somit potenziell auch ungewollte Eskalationsspiralen in Gang setzen könnten, gelte es dabei jedoch zu bedenken. Gestärkt werden könnten hierdurch jedoch auch die europäischen Attributionskapazitäten, um die Anwendung der Cyber Diplomacy Toolbox auf von den USA unabhängigere Füße zu stellen.

Auch auf der noch technischeren Ebene ergeben sich aus den empirischen Ausführungen der Arbeit weitere Policy-Implikationen: Eine internationale Malware-Plattform, in die Länderbehörden Informationen über Vorfälle einspeisen und auf die auch (vorher zertifizierte und regelmäßig überprüfte) private IT-Unternehmen Zugriff haben, könnte dabei helfen, eine ›Cyberpandemie‹ wie NotPetya oder WannaCry in Zukunft zu verhindern bzw. zumindest schneller einzudämmen. Es müsste sich somit um eine Art Frühwarnsystem handeln, das jedoch effektiver funktioniert als bislang bereits bestehende Versuche in diesem Bereich. Es existieren jedoch auch Vorbehalte gegenüber dem Austausch von Malware-Samples z.B. auf VirusTotal, da dies bereits jetzt laut IT-ExpertInnen diverse Risiken für »Intrusion-Detection«- und »-Prevention«-Vorgänge sowie für die betroffenen AkteurInnen birgt. Denn durch das Hochladen der Malware-Samples können Personen mit Zugriffsrechten hierauf potenziell erkennen,

wer von dieser Malware betroffen war, wie der Exploit funktioniert und ggf. auch Einsicht in sensitive Informationen nehmen, falls diese Teil des Samples waren (vgl. Steffens 2020, S. 58). Es käme hier somit auf ein hinreichend vertrauensvolles Netzwerk an zertifizierten AkteurInnen an und zudem auf eine kontrollierte, standardisierte Form der Malware-Veröffentlichung, die den betroffenen AkteurInnen nicht zum Nachteil gereicht. Die Einbindung von Unternehmen in autokratischen Ländern impliziert stets die Gefahr der Weitergabe der technischen Informationen an staatliche Stellen. Wenn jedoch die zunehmende Fragmentierung des Internets aus demokratischer Sicht verhindert werden soll, stellen eben auch alle an das Internet angeschlossenen Systeme in Autokratien Teile der globalen Verwundbarkeitskette dar, die es somit ebenfalls zu stärken gilt. Im Sinne der Arbeit wäre hier zu verhindern, dass im Rahmen dieses Informationsaustauschs autokratische IT-Unternehmen zu den Proxys ihrer Regierungen werden und somit den eigentlichen Zweck des Arrangements unterwandern könnten.

Das Beispiel der israelischen NSO-Group hat ferner gezeigt, dass eine effektivere Kontrolle von Exportregeln betreffend Spionage-Software dringend nötig ist. Diese Technologien sollten nur an Länder geliefert werden, die sie nicht zu innerstaatlicher Repression/Überwachung (aus)nutzen. Dass dies auch Mitgliedstaaten der EU sein können, zeigten die Enthüllungen um den Missbrauch der Pegasus-Software in Spanien, Polen und Ungarn. Demokratische Technologie-Exportländer wie Israel sollten ihren Status nicht zur Erreichung außenpolitischer Ziele instrumentalisieren, sofern dadurch der ideelle Grundkonsens demokratischer Staaten unterminiert wird. Die Regulation des Exports potenziell schadhafter Software sollte zudem trotz bestehender Herausforderungen durch Dual-Use-Technologien allgemein gestärkt werden. Diverse Forschungsarbeiten der letzten Jahre haben sich zunehmend hiermit auseinandergesetzt und z.B. Modelle vorgeschlagen, um die Bewertung einer Software als ›Cyberwaffe‹ bereits *vor* deren Nutzung zu ermöglichen (vgl. Reinhold und Reuter 2021). Weitere seitens der Forschung diskutierte Regulationsmöglichkeiten im offensiven Cyberbereich stellen u.a. die Überlegungen zu einem ›International Vulnerabilities Equities Process‹ (IVEP) dar (Schulze 2020). Die dabei betonte Einschränkung des Nutzens einer Fokussierung auf Zero-Day-Exploits, da dies nur einen kleinen Teil aller Cyberoperationen beträfe, wird auch seitens des HD-CY.CON bestätigt, der lediglich in 38 der 1265 erfassten Fälle berichtete Zero-Days kodiert hat. Regulierungsbemühungen sollten sich somit vor allem auch auf ›Alltags-N-Day-Lücken‹ konzentrieren, die bereits bekannt sind, aus unterschiedlichen Gründen jedoch immer noch von zahlreichen AngreiferInnen gegen verschiedene Zielsysteme ausgenutzt werden können (Beispiel: WannaCry 2017).

Literaturverzeichnis

360Helios (2016): Operation Mermaid. Hg. v. 360 Core Security. Online verfügbar unter https://blogs.360.cn/post/operation-mermaid.html, zuletzt aktualisiert am 30.05.2016, zuletzt geprüft am 01.09.2021.

Achmatova, Nina (2012): Former oligarch appeals to the Patriarch for regime change in Russia. Hg. v. AsiaNews.it. Online verfügbar unter http://www.asianews.it/news-en/Former-oligarch-appeals-to-the-Patriarch-for-regime-change-in-Russia-23726.html, zuletzt aktualisiert am 18.01.2012, zuletzt geprüft am 29.04.2021.

Adams, Gordon; Williams, Cindy (2010): Buying national security: How America plans and pays for Its global role and safety at home. New York: Routledge.

Adamsky, Dmitry (2017): The Israeli Odyssey toward its National Cyber Security Strategy. In: The Washington Quarterly 40 (2), S. 113–127. DOI: 10.1080/0163660X.2017.1328928.

Agrafiotis, Ioannis; Bada, Maria; Cornish, Paul; Creese, Sadie; Goldsmith, Michael; Ignatuschtschenko, Eva et al. (2016): Cyber Harm: Concepts, Taxonomy and Measurement. Hg. v. SAID Business School. University of Oxford (Saïd Business School RP, 2016–23). Online verfügbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828646.

Agrafiotis, Ioannis; Nurse, Jason R. C.; Goldsmith, Michael; Creese, Sadie; Upton, David (2018): A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. In: J Cyber Secur 4 (1). DOI: 10.1093/cybsec/tyy006.

Albert, Eleanor; Maizland, Lindsay; Xu, Beina (2021): The Chinese Communist Party. Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/backgrounder/chinese-communist-party, zuletzt aktualisiert am 23.06.2021, zuletzt geprüft am 09.07.2021.

Alekseyeva, Anna (2015): The Russian politics of multiculturalism | openDemocracy. Hg. v. OpenDemocracy. Online verfügbar unter https://www.opendemocracy.net/en/odr/russian-politics-of-multiculturalism/, zuletzt aktualisiert am 30.03.2015, zuletzt geprüft am 05.05.2021.

Ali, Idrees; Stewart, Phil (2019): Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials. Hg. v. Reuters. Online verfügbar un-

ter https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive-idUSKBN1WV0EK, zuletzt aktualisiert am 16.10.2019, zuletzt geprüft am 06.10.2021.

Alperovitch, Dmitri (2016): Bears in the Midst: Intrusion into the Democratic National Committee. Hg. v. CrowdStrike. Online verfügbar unter https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/, zuletzt geprüft am 15.12.2019.

Al-qatari, Hussain; Gambrell, Jon (2018): Iraq, Saddam and the 1991 Gulf War looms large over George H.W. Bush's legacy. Hg. v. Chicago Tribune. Online verfügbar unter https://www.chicagotribune.com/nation-world/ct-gulf-war-bush-legacy-20181201-story.html, zuletzt aktualisiert am 01.12.2018, zuletzt geprüft am 01.09.2021.

Al-Rawi; Ahmed K. (2014): Cyber warriors in the Middle East: The case of the Syrian Electronic Army. In: Public Relations Review 40 (3), S. 420–428. DOI: 10.1016/j.pubrev.2014.04.005.

Amos, Howard (2017): Vladimir Putin's man in the Balkans. Hg. v. Politico. Online verfügbar unter https://www.politico.eu/article/vladimir-putin-balkans-point-man-nikolai-patrushev/, zuletzt aktualisiert am 21.06.2017, zuletzt geprüft am 12.05.2021.

Anderlini, Jamil (2010): The Chinese dissident's ›unknown visitors‹. Hg. v. Financial Times. Online verfügbar unter https://www.ft.com/content/c590cdd0-016a-11df-8c54-00144feabdc0, zuletzt aktualisiert am 15.01.2010, zuletzt geprüft am 21.06.2021.

Anderson, Collin; Sadjadpour, Karim (2018): Iran's Cyber Threat: Espionage, Sabotage, and Revenge. Washington, D.C.: Carnegie Endowment for International Peace.

Andress, Jason (2014): The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Oxford: Syngress.

Appelbaum, Jacob; Gibson, Aaron, Guarnieri, Claudio; Müller-Maguhn, Andy; Poitras, Laura; Rosenbach, Marcel; Ryge, Leif et al. (2015): Die NSA rüstet zum Cyber-Feldzug. Hg. v. Spiegel Online. Online verfügbar unter https://www.spiegel.de/netzwelt/netzpolitik/snowden-dokumente-wie-die-nsa-digitale-kriege-vorbereitet-a-1013521.html, zuletzt aktualisiert am 18.01.2015, zuletzt geprüft am 10.12.2021.

Applegate, Scott (2011): Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare. In: IEEE Secur. Privacy Mag. 9 (5), S. 16–22. DOI: 10.1109/MSP.2011.46.

Apuzzo, Matt; LaFraniere, Sharon (2018): 13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign. Hg. v. The New York Times, zuletzt aktualisiert am 16.02.2018, zuletzt geprüft am 20.08.2021.

Arquilla, John (2012): Cool War. Foreign Policy. Online verfügbar unter https://foreignpolicy.com/2012/06/15/cool-war/, zuletzt aktualisiert am 15.06.2012, zuletzt geprüft am 25.06.2020.

Asher-dotan, Lital (2018): What Israel's Elite Defense Force Unit 8200 Can Teach Security about Diversity. Hg. v. Dark Reading. Online verfügbar unter https://www.darkreading.com/threat-intelligence/what-israel-s-elite-defense-force-unit-8200-can-teach-security-about-diversity, zuletzt aktualisiert am 21.05.2018, zuletzt geprüft am 25.10.2021.

Associated Press (2021): China tightens political control of internet giants. Hg. v. Politico. Online verfügbar unter https://www.politico.com/news/2021/10/03/china-control-internet-giants-514970, zuletzt aktualisiert am 03.10.2021, zuletzt geprüft am 11.10.2021.

Austin, Greg (2015): How China's Ministry of Public Security Controls Cyber Policy. Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2015/04/how-chinas-ministry-of-public-security-controls-cyber-policy/, zuletzt aktualisiert am 29.04.2015, zuletzt geprüft am 31.07.2021.

Austin, Greg (2016): International Legal Norms in Cyberspace: Evolution of China's National Security Motivations171CHAPTER 9International Legal Norms in Cyberspace: Evolution of China's National Security Motivations. In: Anna-Maria Osula und Henry Rõigas (Hg.): International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn, Estonia: NATO CCD COE Publications, S. 171–201. Online verfügbar unter https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch9.pdf.

Au-Yeung, Angel (2019): What We Know About CrowdStrike, The Cybersecurity Firm Trump Mentioned In Ukraine Call, And Its Billionaire CEO. Hg. v. Forbes. Online verfügbar unter https://www.forbes.com/sites/angelauyeung/2019/09/25/what-we-know-about-crowdstrike-the-cybersecurity-firm-mentioned-by-trump-in-his-call-with-ukraines-president-and-its-billionaire-ceo/?sh=65bbd8321c55, zuletzt aktualisiert am 26.09.2019, zuletzt geprüft am 20.08.2021.

Axelrod, Robert; Iliev, Rumen (2014): Timing of cyber conflict. In: Proceedings of the National Academy of Sciences of the United States of America 111 (4), S. 1298–1303. DOI: 10.1073/pnas.1322638111.

Babayan, Nelli (2015): The return of the empire? Russia's counteraction to transatlantic democracy promotion in its near abroad. In: Democratization 22 (3), S. 438–458. DOI: 10.1080/13510347.2014.993973.

Bachner, Michael (2020): Israeli websites hacked in cyberattack: ›Be ready for a big surprise‹. Hg. v. Times of Israel. Online verfügbar unter https://www.timesofisrael.com/israeli-websites-hacked-in-cyberattack-be-ready-for-a-big-surprise/, zuletzt aktualisiert am 21.05.2020, zuletzt geprüft am 12.02.2022.

Bajak, Frank (2019): Why Trump asked Ukraine's president about ›CrowdStrike‹. Hg. v. Associated Press. Online verfügbar unter https://apnews.com/article/trump-impeachment-inquiry-donald-trump-ap-top-news-politics-technology-aa1f66a1770d4995a6bada960a7d119e, zuletzt aktualisiert am 18.10.2019, zuletzt geprüft am 20.08.2021.

Balding, Christopher (2019): Huawei Technologies' Links to Chinese State Security Services. In: SSRN Journal. DOI: 10.2139/ssrn.3415726.

Ball, Desmond (2011): China's cyber warfare capabilities. In: Security Challenges 7 (2), S. 81–103.

Balmforth, Tom; Tsvetkova, Maria (2022): Russia takes down REvil hacking group at U.S. request – FSB. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/, zuletzt aktualisiert am 14.01.2022, zuletzt geprüft am 24.01.2022.

Banse, Dirk (2009): Putins Konjunkturprogramm: Russische Agenten spionieren deutsche Energie-Unternehmen aus. Hg. v. Welt. Online verfügbar unter https://www.welt.de/wams_print/article3965455/Putins-Konjunkturprogramm-Russische-Agenten-spionieren-deutsche-Energie-Unternehmen-aus.html, zuletzt aktualisiert am 21.06.2009, zuletzt geprüft am 06.05.2021.

Bar, Tomer; Conant, Simon (2016): Infy Malware Active In Decade of Targeted Attacks. Hg. v. Palo Alto Networks. Online verfügbar unter https://unit42.paloaltonetworks.com/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/, zuletzt aktualisiert am 02.05.2016, zuletzt geprüft am 01.09.2021.

Baram, Gil (2017): Israeli defense in the age of cyber war. In: Middle East Quarterly, S. 1–10.

Baram, Gil; Sommer, Udi (2019): Covert or not Covert: National Strategies During Cyber Conflicts. In: T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga und G. Visky (Hg.): 11th International Conference on Cyber Conflict: Silent Battle. Tallinn: NATO CCD COE Publications, S. 197–212.

Barboza, David (2012): Family of Wen Jiabao Holds a Hidden Fortune in China. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2012/10/26/business/global/family-of-wen-jiabao-holds-a-hidden-fortune-in-china.html?pagewanted=all, zuletzt aktualisiert am 25.10.2012, zuletzt geprüft am 02.08.2021.

Bar-eli, Avi (2021): Israel exports arms endangering human rights because it serves our interests, top defense official admits. Hg. v. Haaretz. Online verfügbar unter https://www.haaretz.com/israel-news/.premium.HIGHLIGHT.MAGAZINE-israel-exported-arms-that-endangered-human-rights-top-defense-official-admits-1.10445867, zuletzt aktualisiert am 07.12.2021, zuletzt geprüft am 06.01.2022.

Barlow, John Perry (1996): A Declaration of the Independence of Cyberspace. Hg. v. Electronic Frontier Foundation. Davos. Online verfügbar unter https://www.eff.org/cyberspace-independence, zuletzt aktualisiert am 07.04.2018, zuletzt geprüft am 09.06.2020.

Barnes, Julian E.; Gibbons-Neff, Thomas (2019): U.S. Carried Out Cyberattacks on Iran. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html, zuletzt aktualisiert am 22.06.2019, zuletzt geprüft am 03.01.2022.

Barr, Luke; Margolin, Josh (2022): DHS warns of Russian cyberattack on US if it responds to Ukraine invasion. Hg. v. ABC News. Online verfügbar unter https://abcnews.go.com/Politics/dhs-warns-russian-cyberattack-us-responds-ukraine-invasion/story?id=82441727, zuletzt aktualisiert am 24.01.2022, zuletzt geprüft am 10.02.2022.

Barrett, Brian (2018): How China's Elite APT10 Hackers Stole the World's Secrets. Hg. v. Wired. Online verfügbar unter https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/?redirectURL=https%3A%2F%2Fwww.wired.com%2Fstory%2Fdoj-indictment-chinese-hackers-apt10%2F, zuletzt aktualisiert am 20.12.2018, zuletzt geprüft am 17.06.2021.

Barry, Rob; Volz, Dustin (2019): Ghosts in the Clouds: Inside China's Major Corporate Hack. Hg. v. Wall Street Journal. Online verfügbar unter https://robbarry.org/assets/pdfs/Ghosts%20in%20the%20Clouds.pdf, zuletzt aktualisiert am 30.12.2019, zuletzt geprüft am 29.12.2021.

Bar-Siman-Tov, Yaacov (1984): The strategy of war by proxy. In: Cooperation and Conflict 19 (4), S. 263–273.

Bartholomew, Brian; Guerrero-Saade, Juan Andres (2016): Wave your flags! Deception tactics muddying attribution in targeted attacks. q. Hg. v. Virus Bulletin Conference.

Bartlett, Jason (2020): Exposing the Financial Footprints of North Korea's Hackers. Hg. v. Center for a new Amercian Security. Online verfügbar unter https://www.cnas.org/publications/reports/exposing-the-financial-footprints-of-north-koreas-hackers, zuletzt aktualisiert am 18.11.2020, zuletzt geprüft am 08.02.2021.

Bättig, Michèle B.; Bernauer, Thomas (2009): National institutions and global public goods: are democracies more cooperative in climate change policy? In: International Organization, S. 281–308.

Baumgartner, Kurt; Garnaeva, Maria (2014): BE2 custom plugins, router abuse, and target profiles. Hg. v. Securelist. Kaspersky. Online verfügbar unter https://securelist.com/be2-custom-plugins-router-abuse-and-target-profiles/67353/, zuletzt aktualisiert am 03.11.2014, zuletzt geprüft am 18.04.2021.

BBC (2012): ›Hacking attacks‹ hit Russian political sites. Hg. v. BBC. Online verfügbar unter https://www.bbc.com/news/technology-16032402?print=true, zuletzt aktualisiert am 08.03.2012, zuletzt geprüft am 04.05.2021.

BBC (2016): Chinese hackers turn to ransomware. Hg. v. BBC. Online verfügbar unter https://www.bbc.com/news/technology-35811777, zuletzt aktualisiert am 15.03.2016, zuletzt geprüft am 17.06.2021.

Beaumont, Peter (2016): US abstention allows UN to demand end to Israeli settlements. Hg. v. The Guardian, zuletzt aktualisiert am 23.12.2016, zuletzt geprüft am 05.01.2022.

Behar, Richard (2016): Inside Israel's Secret Startup Machine. Hg. v. Forbes. Online verfügbar unter https://www.forbes.com/sites/richardbehar/2016/05/11/inside-israels-secret-startup-machine/?sh=27c295f61a51, zuletzt aktualisiert am 30.05.2016, zuletzt geprüft am 11.10.2021.

Bejtlich, Richard (2014): DoJ Indicts Chinese Military Hackers: First Impressions. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/blog/executive-perspective/2014/05/doj-indicts-chinese-military-hackers-first-impressions.html, zuletzt aktualisiert am 20.05.2014, zuletzt geprüft am 12.08.2021.

Bendiek, Annegret; Schulze, Matthias (2021): Attribution als Herausforderung für EU-Cybersanktionen. Hg. v. Stiftung Wissenschaft Und Politik. Online verfügbar unter https://www.swp-berlin.org/publikation/attribution-als-herausforderung-fuer-eu-cybersanktionen.

Ben-Eliezer, Uri (2001): From Military Role-Expansion to Difficulties in Peace-Making: The Israel Defense Forces 50 Years on.«. In: Military, State and Society in Israel: Theoretical and Comparative Perspective, S. 137–172.

Benjakob, Omer; Yaron, Oded (2021): Substantial majority of Jewish Israelis feel unregulated cyberarm sales are ›immoral‹. Hg. v. Haaretz. Online verfügbar unter https://www.haaretz.com/israel-news/tech-news/.premium-majority-of-jewish-israelis-feel-unregulated-cyberarm-sales-are-immoral-1.10102292, zuletzt aktualisiert am 09.08.2021, zuletzt geprüft am 03.01.2022.

Benjamin, Henry (2011): Radware – Cyber Soldiers. Hg. v. J-Wire. Online verfügbar unter https://www.jwire.com.au/radware-cyber-soldiers/, zuletzt aktualisiert am 27.11.2011, zuletzt geprüft am 11.10.2021.

Benn, Aluf (2009): Why isn't Netanyahu backing two-state solution? Hg. v. Haaretz. Online verfügbar unter https://www.haaretz.com/1.5081572, zuletzt aktualisiert am 01.03.2009, zuletzt geprüft am 05.01.2022.

Bennett, Andrew (2004): Case study methods: Design, use, and comparative advantages. In: Detlef F. Sprinz und Yael Wolinsky-Nahmias (Hg.): Models, numbers, and cases. Methods for studying international relations. [Nachdr.]. Ann Arbor, Mich.: Univ. of Michigan Press, S. 19–55.

Ben-Porat, Guy (2005): Netanyahu's second coming: A neoconservative policy paradigm? In: Israel Studies 10 (3), S. 225–245.

Berghel, Hal (2017): On the Problem of (Cyber) Attribution. In: Computer 50 (3), S. 84–89. DOI: 10.1109/MC.2017.74.

Bergman, Michael K. (2001): White Paper: The Deep Web: Surfacing Hidden Value. In: The Journal of Electronic Publishing 7 (1). DOI: 10.3998/3336451.0007.104.

Bergman, Ronen (2019): Rise and Kill First: The Secret History of Israel's Targeted Assassinations. New York: Random House.

Bergmann, Max; Cicarelli, Siena (2021): NATO's Financing Gap. Hg. v. Center for American Progress. Online verfügbar unter https://www.americanprogress.org/article/natos-financing-gap/, zuletzt aktualisiert am 13.01.2021, zuletzt geprüft am 02.01.2022.

Bettiza, Gregorio; Lewis, David (2020): Authoritarian Powers and Norm Contestation in the Liberal International Order: Theorizing the Power Politics of Ideas and Identity. In: Journal of Global Security Studies 5 (4), S. 559–577. DOI: 10.1093/jogss/ogz075.

Betts, Richard K. (2007): Two Faces of Intelligence Failure: September 11 and Iraq's Missing WMD. In: Political Science Quarterly 122 (4), S. 585–606. Online verfügbar unter http://www.jstor.org/stable/20202928.

Beuth, Patrick; Biermann, Kai; Klingst, Martin; Stark, Holger (2017): Bundestags-Hack: So wurde das deutsche Parlament ausspioniert. Hg. v. Die Zeit. Online verfügbar unter https://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland?utm_referrer=https%3A%2F%2Fwww.google.com%2F, zuletzt aktualisiert am 11.05.2017, zuletzt geprüft am 18.04.2021.

BfV (2019): BfV Cyber – Brief Nr. 01/2019. Hinweis auf aktuelle Angriffskampagne. Hg. v. Bundesamt für Verfassungsschutz (BfV). Online verfügbar unter http://docs.dpaq.de/15627-cyber-brief_nr-6_06-12-19.pdf, zuletzt geprüft am 25.06.2021.

Bhattacharya, Abanti (2019): Chinese Nationalism Under Xi Jinping Revisited. In: India Quarterly 75 (2), S. 245–252. DOI: 10.1177/0974928419841789.

Biasini, Nick; Chen, Michael; Karkins, Alex; Khodjibaev, Azim; Neal, Chris; Olney, Matt (2022): Comprehensive Threat Intelligence: Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation. Hg. v. Talos. Online verfügbar unter https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html, zuletzt aktualisiert am 04.02.2022, zuletzt geprüft am 10.02.2022.

Bing, Chris (2017a): Security firms sometimes wreck FBI investigations. Here's how. Hg. v. Cyberscoop. Online verfügbar unter https://www.cyberscoop.com/security-researchers-occasionally-disrupt-fbi-investigations-heres-how/, zuletzt aktualisiert am 03.04.2017, zuletzt geprüft am 12.08.2021.

Bing, Chris (2017b): Ukraine blames infamous Russian hackers for ›BadRabbit‹ ransomware attack. Hg. v. Cyberscoop. Online verfügbar unter https://www.cyberscoop.com/fancy-bear-bad-rabbit-ransomware-security-service-of-ukraine/, zuletzt aktualisiert am 02.11.2017, zuletzt geprüft am 01.01.2022.

Bing, Chris (2018): China's government is keeping its security researchers from attending conferences. Hg. v. Cyberscoop. Online verfügbar unter https://www.cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/, zuletzt aktualisiert am 08.03.2018, zuletzt geprüft am 25.10.2021.

Bing, Christopher (2021): White House blames Russian spy agency SVR for SolarWinds hack: statement. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/business/white-house-blames-russian-spy-agency-svr-solarwinds-hack-statement-2021-04-15/, zuletzt aktualisiert am 15.04.2021, zuletzt geprüft am 12.05.2021.

Bing, Christopher; Taylor, Marisa (2020): Exclusive: China-backed hackers ›targeted COVID-19 vaccine firm Moderna‹. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-health-coronavirus-moderna-cyber-excl-idUSKCN24V38M, zuletzt aktualisiert am 30.07.2020.

Bisson, David (2018): New Gallmaker Attack Group Using Living-off-the-Land Tactics in Espionage Campaign. Hg. v. Security Intelligence. Online verfügbar unter https://securityintelligence.com/news/new-gallmaker-attack-group-using-living-off-the-land-tactics-in-espionage-campaign/, zuletzt aktualisiert am 19.10.2018.

Bitton, Raphael (2016): In law we trust: the Israeli case of overseeing intelligence. In: Zachary K. Goldman und Samuel James Rascoff (Hg.): Global intelligence oversight. Governing security in the twenty-first century. New York: Oxford University Press, S. 141–174.

Blank, Stephen (2017): Cyber and Information War à la Russe. In: George Perkovich und Ariel E. Levite (Hg.): Understanding cyber conflict. 14 analogies. Washington, D.C.: Georgetown University Press, S. 81–98.

Bloomberg News (2012): Xi Jinping Millionaire Relations Reveal Fortunes of Elite. Hg. v. Bloomberg. Online verfügbar unter https://www.bloomberg.com/news/articles/2012-06-29/xi-jinping-millionaire-relations-reveal-fortunes-of-elite, zuletzt aktualisiert am 29.06.2012, zuletzt geprüft am 02.08.2021.

Bob, Yonah Jeremy (2016): Islamic Jihad cyber terrorist indicted for hacking IDF drones over Gaza. Hg. v. The Jerusalem Post. Online verfügbar unter https://www.jpost.com/Arab-Israeli-Conflict/Islamic-Jihad-cyber-terrorist-indicted-for-hacking-IDF-drones-over-Gaza-448936, zuletzt aktualisiert am 23.03.2016, zuletzt geprüft am 06.01.2022.

Bob, Yonah Jeremy (2021): New Shin Bet head: Ready to take on Iran, Israeli-Arab violence. Hg. v. The Jerusalem Post. Online verfügbar unter https://www.jpost.com/middle-east/iran-news/new-shin-bet-head-ready-to-take-on-iran-israeli-arab-violence-681866, zuletzt aktualisiert am 13.10.2021, zuletzt geprüft am 06.01.2022.

Bodeen, Christopher (2007): New Chinese spy chief an expert on commercial intelligence, monitoring group says. Hg. v. Taiwan News. Online verfügbar unter https://www.taiwannews.com.tw/en/news/512740, zuletzt aktualisiert am 31.08.2007, zuletzt geprüft am 31.07.2021.

Boehm, Dana Carver (2009): China's Failed War on Terror: Fanning the Flames of Uighur Separatist Violence. In: Berkeley J. Middle E. & Islamic L. 2, S. 61.

Boeke, Sergei; Broeders, Dennis (2018): The Demilitarisation of Cyber Conflict. In: Survival 60 (6), S. 73–90. DOI: 10.1080/00396338.2018.1542804.

Borger, Julian (2006): Neocons turn on Bush for incompetence over Iraq war. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2006/nov/04/iraq.midterms2006, zuletzt aktualisiert am 04.11.2006, zuletzt geprüft am 26.08.2021.

Borghard, Erica D. (2021): Time to End the Dual Hat? Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/blog/time-end-dual-hat, zuletzt aktualisiert am 03.02.2021, zuletzt geprüft am 24.08.2021.

Borghard, Erica D.; Lonergan, Shawn W. (2016): Can States Calculate the Risks of Using Cyber Proxies? In: Orbis 60 (3), S. 395–416. DOI: 10.1016/j.orbis.2016.05.009.

Borghard, Erica D.; Lonergan, Shawn W. (2017): The Logic of Coercion in Cyberspace. In: Security Studies 26 (3), S. 452–481. DOI: 10.1080/09636412.2017.1306396.

Borghard, Erica D.; Lonergan, Shawn W. (2018): What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations? Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations, zuletzt aktualisiert am 10.09.2018, zuletzt geprüft am 24.08.2021.

Borghard, Erica D.; Lonergan, Shawn W. (2019): Cyber Operations as Imperfect Tools of Escalation. In: Strategic Studies Quarterly 13 (3), S. 122–145.

Bowen, Andrew S. (2021): Russian Cyber Units. Hg. v. Congressional Research Service (In Focus, IF11718). Online verfügbar unter https://crsreports.congress.gov/product/pdf/IF/IF11718, zuletzt geprüft am 14.04.2021.

Bradbury, Danny (2019): FSB hackers drop files online. Hg. v. Naked Security. Online verfügbar unter https://nakedsecurity.sophos.com/2019/07/23/fsb-hackers-drop-files-online/, zuletzt aktualisiert am 23.07.2019, zuletzt geprüft am 20.05.2021.

Branigan, Tania (2009): China restores limited internet access after Urumqi violence. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2009/jul/28/china-restores-limited-internet-access, zuletzt aktualisiert am 28.07.2009, zuletzt geprüft am 27.07.2021.

Branigan, Tania; Halliday, Josh (2011): China hits back over US claims of satellite hacking. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/technology/2011/oct/31/china-us-claims-satellite-hacking, zuletzt aktualisiert am 31.10.2011, zuletzt geprüft am 29.07.2021.

Brantly, Aaron F. (2014): Cyber Actions by State Actors: Motivation and Utility. In: International Journal of Intelligence and CounterIntelligence 27 (3), S. 465–484. DOI: 10.1080/08850607.2014.900291.

Breland, Ali (2018): Trump broadens attack on Silicon Valley companies. Hg. v. The Hill. Online verfügbar unter https://thehill.com/policy/technology/404042-trump-broadens-attack-on-silicon-valley-companies, zuletzt aktualisiert am 28.08.2018, zuletzt geprüft am 02.09.2021.

Bremmer, Ian; Charap, Samuel (2007): The siloviki in Putin's Russia: who they are and what they want. In: The Washington Quarterly 30 (1), S. 83–92.

Brenner, Susan W. (2007): At light speed: attribution and response to cybercrime/terrorism/warfare. In: Journal of Criminal Law and Criminology 97 (2), S. 379–475.
Brewster, Thomas (2016a): Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text. Hg. v. Forbes. Online verfügbar unter https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/?sh=355b22d63997, zuletzt aktualisiert am 26.08.2016, zuletzt geprüft am 26.10.2021.
Brewster, Thomas (2016b): Ukraine Claims Hackers Caused Christmas Power Outage. Hg. v. Forbes. Online verfügbar unter https://www.forbes.com/sites/thomasbrewster/2016/01/04/ukraine-power-out-cyber-attack/?sh=56bb54836fa8, zuletzt aktualisiert am 04.01.2016, zuletzt geprüft am 18.04.2021.
Brichta, Avraham (1998): The new premier-parliamentary system in Israel. In: The Annals of the American Academy of Political and Social Science 555 (1), S. 180–192.
Broadhurst, Rod; Grabosky, Peter (2005): Cyber-crime: The challenge in Asia. Hong Kong: Hong Kong University Press.
Broadhurst, Roderic; Grabosky, Peter; Alazab, Mamoun; Bouhours, Brigitte; Chon, Steve (2014): An analysis of the nature of groups engaged in cyber crime. In: International Journal of Cyber Criminology 8 (1), S. 1–20.
Bronk, Christopher; Tikk-Ringas, Eneken (2013): Hack or attack? Shamoon and the Evolution of Cyber Conflict. Hg. v. James A. Baker III Institute for Public Policy. Rice University. Online verfügbar unter https://scholarship.rice.edu/bitstream/handle/1911/92672/ITP-pub-WorkingPaper-ShamoonCyberConflict-020113.pdf?sequence=1, zuletzt aktualisiert am 2013, zuletzt geprüft am 03.06.2020.
Brooks, Risa (2021): Through the Looking Glass: Trump-Era Civil-Military Relations in Comparative Perspective. In: Strategic Studies Quarterly 15 (2).
Brosgol, Dan (2019): Passover 5779: In Every Generation. Hg. v. The Bedford Citizen. Online verfügbar unter https://www.thebedfordcitizen.org/2019/04/passover-5779-in-every-generation/, zuletzt aktualisiert am 18.04.2019, zuletzt geprüft am 03.01.2022.
Brown, Kerry; Bērziņa-Čerenkova, Una Aleksandra (2018): Ideology in the Era of Xi Jinping. In: Journal of Chinese Political Science 23 (3), S. 323–339. DOI: 10.1007/s11366-018-9541-z.
BSI (2021): Social Engineering – der Mensch als Schwachstelle. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html, zuletzt aktualisiert am 21.05.2021, zuletzt geprüft am 17.01.2022.
Buchanan, Ben (2017): The cybersecurity dilemma. Hacking, trust and fear between nations. New York, NY: Oxford University Press.
Buckley, Noah; Reuter, Ora John (2019): Performance Incentives under Autocracy: Evidence from Russia's Regions. In: Comparative Politics 51 (2), S. 239–266. DOI: 10.5129/001041519X15647434969894.
Bugos, Shannon (2019): U.S. Completes INF Treaty Withdrawal | Arms Control Association. Hg. v. Arms Control Association. Online verfügbar unter https://www.armscon

trol.org/act/2019-09/news/us-completes-inf-treaty-withdrawal, zuletzt aktualisiert am 09.2019, zuletzt geprüft am 06.10.2021.
Bukkvoll, Tor; Østensen, Åse G. (2020): The Emergence of Russian Private Military Companies: A New Tool of Clandestine Warfare. In: Special Operations Journal 6 (1), S. 1–17. DOI: 10.1080/23296151.2020.1740528.
Burnell, Peter (2006): Autocratic opening to democracy: why legitimacy matters. In: Third World Quarterly 27 (4), S. 545–562.
Butt, Ahsan I. (2019): Why did Bush go to war in Iraq? Hg. v. Aj Jazeera. Online verfügbar unter https://www.aljazeera.com/opinions/2019/3/20/why-did-bush-go-to-war-in-iraq, zuletzt aktualisiert am 20.03.2019, zuletzt geprüft am 01.09.2021.
Cabestan, Jean-Pierre (2009): China's foreign-and security-policy decision-making processes under Hu Jintao. In: Journal of Current Chinese Affairs 38 (3), S. 63–97.
Calabresi, Massimo (2017): The Secret History of an Election. In: TIME Magazine 190 (5), S. 32–39.
Calian (2020): The Breach Report – Issue 8. Hg. v. Calian. Online verfügbar unter https://www.calian.com/assets/downloads/The-Breach-Report-Issue-8-Scandalous-Hacking-Operation.pdf, zuletzt geprüft am 12.11.2021.
Canfil, Justin Key (2016): Honing Cyber Attribution. The Cyber Issue. In: Journal of International Affairs 70 (1), S. 217–226.
Canfil, Justin Key (2020): Outsourcing Cyber Power: Why Proxy Conflict in Cyberspace May No Longer Pay. Hg. v. SSRN. Online verfügbar unter https://ssrn.com/abstract=3611582, zuletzt geprüft am 27.04.2021.
Carmola, Kateri (2010): Private security contractors and new wars: risk, law, and ethics: Routledge.
Carnegie, Allison; Carson, Austin (2020): Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation: Cambridge University Press.
Carothers, Thomas (2007): US Democracy Promotion During and after Bush 2007. Hg. v. Carnegie Endowment for International Peace. Online verfügbar unter https://carnegieendowment.org/files/democracy_promotion_after_bush_final.pdf, zuletzt geprüft am 01.09.2021.
Carr, Jeffrey (2011): Inside cyber warfare. Mapping the cyber underworld. 2. Aufl. Sebastopol, CA: O'Reilly & Associates.
Carson, Austin; Yarhi-Milo, Keren (2017): Covert Communication: The Intelligibility and Credibility of Signaling in Secret. In: Security Studies 26 (1), S. 124–156. DOI: 10.1080/09636412.2017.1243921.
CBS News (2014): North Korea blames U.S. for Internet shutdown. Hg. v. CBS News. Online verfügbar unter https://www.cbsnews.com/news/north-korea-blames-u-s-for-internet-shutdown/, zuletzt aktualisiert am 27.12.2014, zuletzt geprüft am 08.09.2021.
CEIC (2021): China Foreign Direct Investment. Hg. v. CEIC. Online verfügbar unter https://www.ceicdata.com/en/indicator/china/foreign-direct-investment, zuletzt geprüft am 29.07.2021.
Cerulus, Laurens (2019): How Ukraine became a test bed for cyberweaponry. Unter Mitarbeit von Politico. Online verfügbar unter https://www.politico.eu/article/ukraine-cy

ber-war-frontline-russia-malware-attacks/, zuletzt aktualisiert am 14.02.2019, zuletzt geprüft am 16.04.2021.

CFR (2020): Cyber Operations Tracker. Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/interactive/cyberoperations.

CFR (2021): Connect the Dots on State-Sponsored Cyber Incidents – Offensive cyber campaign against Georgia. Hg. v. Council on Foreign Relations. Online verfügbar unter https://microsites-live-backend.cfr.org/cyber-operations/offensive-cyber-campaign-against-georgia, zuletzt aktualisiert am 14.04.2021, zuletzt geprüft am 18.04.2021.

Chang, Wu-ueh; Chao, Chien-min (2009): Managing Stability in the Taiwan Strait: Non-Military Policy towards Taiwan under Hu Jintao. In: Journal of Current Chinese Affairs 38 (3), S. 98–118.

Chatzky, Andrew (2020): China's Massive Belt and Road Initiative. Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative, zuletzt aktualisiert am 28.01.2020, zuletzt geprüft am 04.08.2021.

Check Point (2021a): Check Point Company Overview. Hg. v. Check Point. Online verfügbar unter https://www.checkpoint.com/about-us/company-overview/#, zuletzt geprüft am 11.10.2021.

Check Point (2021b): Leadership. Hg. v. Check Point. Online verfügbar unter https://www.checkpoint.com/about-us/leadership/, zuletzt geprüft am 11.10.2021.

Chepikova, Ksenia; Leiße, Olaf (2010): Russlands simulierter Föderalismus: Regionalpolitik unter Putin und Medvedev. In: Osteuropa 60 (1), S. 15–25. Online verfügbar unter https://www.jstor.org/stable/44935441.

Cheravitch, Joe; Lilly, Bilyana (2020): Russia's Cyber Limitations in Personnel and Innovation, Their Potential Impact on Future Operations, and How NATO and Its Members Can Respond. In: A. Ertan, K. Floyd, P. Pernik und S. Stevens (Hg.): Cyber Threats and NATO 2030: Horizon Scanning and Analysis, S. 31–59.

Chernenko, Elena (2015): Terrorism, Ukraine and the American threat: the view from Russia. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2015/jul/15/russia-terrorism-ukraine-america-putin, zuletzt aktualisiert am 15.07.2015, zuletzt geprüft am 12.05.2021.

Cheung, Tai Ming (2017): Xi Takes Charge: Implications of the 19th Party Congress for China's Future. Xi Jinping and the Remaking of Chinese Military Politics. 21st Century China Center. San Diego. Online verfügbar unter https://china.ucsd.edu/_files/2017_xi-briefing-web.pdf, zuletzt geprüft am 25.07.2021.

Chin, Josh (2017): Chinese Firm Behind Alleged Hacking Was Disbanded This Month. Hg. v. The Wall Street Journal. Online verfügbar unter https://www.wsj.com/articles/chinese-firm-behind-alleged-hacking-was-disbanded-this-month-1511881494, zuletzt aktualisiert am 29.11.2017, zuletzt geprüft am 29.06.2021.

China.org (2003): What Is »Three Represents« CPC Theory? Hg. v. China.org. Online verfügbar unter http://www.china.org.cn/english/zhuanti/3represents/68735.htm, zuletzt aktualisiert am 27.11.2003, zuletzt geprüft am 25.07.2021.

China.org (2006): Die 4. Tagung des 10. NVK und des 10. Landeskomitees der PKKCV findet feierlich statt. Hg. v. China.org. Online verfügbar unter http://german.china.o

rg.cn/politics/archive/lianghui06/txt/2006-03/10/content_2225597.htm, zuletzt aktualisiert am 14.12.2006, zuletzt geprüft am 27.07.2021.

Choi, Sung J.; Johnson, M. Eric; Lehmann, Christoph U. (2019): Data breach remediation efforts and their implications for hospital quality. In: Health services research 54 (5), S. 971–980. DOI: 10.1111/1475-6773.13203.

Cimpanu, Catalin (2016): Philippines Government Websites Hit by Massive DDoS Attacks, China Suspected. Hg. v. Softpedia. Online verfügbar unter https://news.softpedia.com/news/philippines-government-websites-hit-by-massive-ddos-attacks-china-suspected-506412.shtml#ixzz4EnloNxmF, zuletzt aktualisiert am 23.06.2021, zuletzt geprüft am 23.06.2021.

Cimpanu, Catalin (2019): In a first, Israel responds to Hamas hackers with an air strike. Hg. v. ZDnet. Online verfügbar unter https://www.zdnet.com/article/in-a-first-israel-responds-to-hamas-hackers-with-an-air-strike/, zuletzt aktualisiert am 05.05.2019, zuletzt geprüft am 13.10.2021.

Cimpanu, Catalin (2021a): China says a foreign spy agency hacked its airlines, stole passenger records. Hg. v. The Record. Online verfügbar unter https://therecord.media/china-says-a-foreign-spy-agency-hacked-its-airlines-stole-passenger-records/, zuletzt aktualisiert am 08.11.2021, zuletzt geprüft am 09.02.2022.

Cimpanu, Catalin (2021b): Japanese police say Tick APT is linked to Chinese military. Hg. v. The Record. Recorded Future. Online verfügbar unter https://therecord.media/japanese-police-say-tick-apt-is-linked-to-chinese-military/, zuletzt aktualisiert am 20.04.2021, zuletzt geprüft am 05.07.2021.

CISA (2018): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Hg. v. Cybersecurity & Infrastructure Security Agency. Online verfügbar unter https://www.cisa.gov/uscert/ncas/alerts/TA18-074A, zuletzt aktualisiert am 16.03.2018, zuletzt geprüft am 01.01.2022.

CISA (2021): Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) | CISA. Hg. v. Cybersecurity & Infrastructure Security Agency. Online verfügbar unter https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure, zuletzt aktualisiert am 01.10.2021, zuletzt geprüft am 01.10.2021.

Clark, David D.; Landau, Susan (2010): Untangling attribution. In: National Research Council (Hg.): Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington, D.C.: The National Academies Press, S. 25–40.

Clayton, Mark (2012): Stealing US business secrets: Experts ID two huge cyber ›gangs‹ in China. Hg. v. The Christian Science Monitor. Online verfügbar unter https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China, zuletzt aktualisiert am 14.09.2012, zuletzt geprüft am 02.07.2021.

Clayton, Mark (2013): Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage. Hg. v. The Christian Science Monitor. Online verfügbar unter https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural

-gas-pipelines-vulnerable-to-sabotage, zuletzt aktualisiert am 27.02.2013, zuletzt geprüft am 25.05.2021.

ClearSky (2020): Operation ›Dream Job‹ Widespread North Korean Espionage Campaign. Hg. v. ClearSky. Online verfügbar unter https://www.clearskysec.com/operation-dream-job/, zuletzt aktualisiert am 13.08.2020, zuletzt geprüft am 12.02.2022.

ClearSky (2021): About ClearSky. Hg. v. ClearSky. Online verfügbar unter https://www.clearskysec.com/company/#block-0, zuletzt geprüft am 11.10.2021.

Cloherty, Jack; Thomas, Pierre (2014): ›Trojan Horse‹ Bug Lurking in Vital US Computers Since 2011. Hg. v. ABC News. Online verfügbar unter https://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476, zuletzt aktualisiert am 06.11.2014, zuletzt geprüft am 06.05.2021.

Clunan, Anne L. (2019): Russia's pursuit of great-power status and security. In: Roger E. Kanet (Hg.): Routledge Handbook of Russian Security. Milton: Routledge, S. 3–16.

Cohen, Stuart A. (2006): Changing Civil–Military Relations in Israel: Towards an Over-subordinate IDF? In: Israel Affairs 12 (4), S. 769–788. DOI: 10.1080/13533310600890091.

Cohen, Zachary (2020): US recently conducted cyber operation against Iran to protect election from foreign interference – CNNPolitics. Hg. v. CNN. Online verfügbar unter https://edition.cnn.com/2020/11/03/politics/us-cyber-operation-iran-election-interference/index.html, zuletzt aktualisiert am 03.11.2020, zuletzt geprüft am 06.10.2021.

Collier, David; Brady, Henry E.; Seawright, Jason (2004): Sources of Leverage in Casual Inference: Toward an Alternative View of Methodology. In: Henry E. Brady und David Collier (Hg.): Rethinking social inquiry. Diverse tools, shared standards. Lanham, Md.: Rowman & Littlefield, S. 229–266.

Collier, Kevin (2018): The Indictment Of North Korea For The Sony Hack Shows How Cybersecurity Has Evolved. Hg. v. BuzzFeed News. Online verfügbar unter https://www.buzzfeednews.com/article/kevincollier/the-indictment-of-north-korea-for-the-sony-hack-shows-how, zuletzt aktualisiert am 08.09.2018, zuletzt geprüft am 11.08.2021.

Collins, Sean; McCombie, Stephen (2012): Stuxnet: the emergence of a new cyber weapon and its implications. In: Journal of Policing, Intelligence and Counter Terrorism 7 (1), S. 80–91. DOI: 10.1080/18335330.2012.653198.

Connell, Michael; Vogler, Sarah (2017): Russia's Approach to Cyber Warfare. Hg. v. CNA. Online verfügbar unter https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf, zuletzt aktualisiert am März 2017, zuletzt geprüft am 10.06.2020.

Cooley, Alexander (2015): Countering Democratic Norms. Journal of Democracy, 26(3), 49–63. DOI: 10.1353/jod.2015.0049.

Cooper, Helene; Barnes, Julian E. (2021): U.S. Considers Warning Ukraine of a Russian Invasion in Real-Time. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2021/12/23/us/politics/russia-ukraine-military-biden.html, zuletzt aktualisiert am 23.12.2021, zuletzt geprüft am 13.01.2022.

Cooper, Cortez A., III (2018): PLA Military Modernization: Drivers, Force Restructuring, and Implications. Hg. v. RAND Corporation. Online verfügbar unter https://www.

rand.org/pubs/testimonies/CT488.html, zuletzt aktualisiert am 15.02.2018, zuletzt geprüft am 02.08.2021.

Copp, Tara (2019): The clash between Trump and his generals. Hg. v. Military Times. Online verfügbar unter https://www.militarytimes.com/news/your-military/2019/01/04/the-clash-between-trump-and-his-generals/, zuletzt aktualisiert am 04.01.2019, zuletzt geprüft am 30.08.2021.

Corbin, Kenneth (2013): Economic Impact of Cyber Espionage and IP Theft Hits U.S. Businesses Hard. Hg. v. CIO. Online verfügbar unter https://www.cio.com/article/2384269/economic-impact-of-cyber-espionage-and-ip-theft-hits-u-s--businesses-hard.html, zuletzt aktualisiert am 10.07.2013, zuletzt geprüft am 02.09.2021.

Cordey, Sean (2019): The Israeli Unit 8200 – An OSINT-based study: Trend Analysis. Unter Mitarbeit von Tim Prior, Myriam Dunn Cavelty und Andreas Wenger. Hg. v. ETH Zürich. Online verfügbar unter https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/389135/Cyber-Reports-2019-12-Unit-8200.pdf?sequence=1&isAllowed=y, zuletzt aktualisiert am 31.12.2019, zuletzt geprüft am 11.10.2019.

Corera, Gordon (2017): Cyber-attack: US and UK blame North Korea for WannaCry. Hg. v. BBC. Online verfügbar unter https://www.bbc.com/news/world-us-canada-42407488, zuletzt aktualisiert am 19.12.2017, zuletzt geprüft am 06.10.2021.

Corera, Gordon (2018): UK think tanks hacked by groups in China, cyber-security firm says. Hg. v. BBC. Online verfügbar unter https://www.bbc.com/news/uk-43172371, zuletzt aktualisiert am 26.02.2018, zuletzt geprüft am 17.06.2021.

Corera, Gordon (2019): Russian hackers cloak attacks using Iranian group. Hg. v. BBC. Online verfügbar unter https://www.bbc.com/news/technology-50103378, zuletzt aktualisiert am 21.10.2019.

Corera, Gordon (2020): Huawei: MPs claim ›clear evidence of collusion‹ with Chinese Communist Party. Hg. v. BBC. Online verfügbar unter https://www.bbc.com/news/technology-54455112, zuletzt aktualisiert am 08.10.2020, zuletzt geprüft am 04.08.2021.

Cormac, Rory; Aldrich, Richard J. (2018): Grey is the new black: covert action and implausible deniability. In: International Affairs 94 (3), S. 477–494.

Costello, John (2016): China's Intelligence Services and Espionage Operations. Hearing before the United States-China Economic and Security Review Commission. Hg. v. United States-China Economic and Security Review Commission. Online verfügbar unter https://www.uscc.gov/sites/default/files/transcripts/June%2009,%202016%20Hearing%20Transcript.pdf, zuletzt aktualisiert am 09.06.2016, zuletzt geprüft am 31.07.2021.

Costello, John; McReynolds, Joe (2018): China's strategic support force: A force for a new era. In: China Strategic Perspective 13.

Cox, Joseph (2018): Meet ›Intrusion Truth,‹ the Mysterious Group Doxing Chinese Intel Hackers. Hg. v. Vice. Online verfügbar unter https://www.vice.com/en/article/wjka84/intrusion-truth-group-doxing-hackers-chinese-intelligence, zuletzt aktualisiert am 21.08.2018, zuletzt geprüft am 29.06.2021.

Crawford, Emily (2013): Virtual Backgrounds: Direct Participation in Cyber Warfare. In: I/S: A Journal of Law and Policy for the Information Society 9 (1), S. 1–19. Online ver-

fügbar unter https://kb.osu.edu/bitstream/handle/1811/73306/1/ISJLP_V9N1_001.pdf, zuletzt geprüft am 18.05.2020.

Cristiano, Fabio (2021): Israel: Cyber Warfare and Security as National Trademarks of International Legitimacy. In: Scott N. Romaniuk und Mary Manjikian (Hg.): Routledge Companion to Global Cyber-Security Strategy. 1. Aufl.: Routledge. Online verfügbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3698972.

Cronin, Patrick (2021): How to Asymmetrically Out-Compete Xi Jinping's One Belt One Road Initiative. Hg. v. War on the Rocks. Online verfügbar unter https://warontherocks.com/2021/03/how-to-asymmetrically-out-compete-xi-jinpings-one-belt-one-road-initiative/, zuletzt aktualisiert am 02.03.2021, zuletzt geprüft am 04.08.2021.

CrowdStrike: 2015 Global Threat Report. Hg. v. Crowdstrike Intelligence Team. CrowdStrike. Online verfügbar unter https://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf?_ga=2.262085646.2058489206.1618905672-118602449.1618212950, zuletzt geprüft am 20.04.2021.

CrowdStrike (2016): Bears in the Midst: Intrusion into the Democratic National Committee. Hg. v. CrowdStrike. Online verfügbar unter https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.06.16.DNC/Bears%20in%20the%20Midst_%20Intrusion%20into%20the%20Democratic%20National%20Committee%20%C2%BB.pdf, zuletzt aktualisiert am 15.06.2016, zuletzt geprüft am 19.04.2021.

CrowdStrike (2020): Our Work with the DNC: Setting the record straight. Hg. v. CrowdStrike. Online verfügbar unter https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/, zuletzt aktualisiert am 05.06.2020, zuletzt geprüft am 14.04.2021.

CrowdStrike (2021a): Cozy Bear. Hg. v. CrowdStrike. Online verfügbar unter https://adversary.crowdstrike.com/adversary/cozy-bear/, zuletzt aktualisiert am 2021, zuletzt geprüft am 14.04.2021.

CrowdStrike (2021b): Venomous Bear. Hg. v. CrowdStrike. Online verfügbar unter https://adversary.crowdstrike.com/adversary/venomous-bear/, zuletzt aktualisiert am 07.04.2021, zuletzt geprüft am 14.04.2021.

Crowley, Michael (2020): Allies and Former U.S. Officials Fear Trump Could Seek NATO Exit in a Second Term. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2020/09/03/us/politics/trump-nato-withdraw.html, zuletzt aktualisiert am 03.09.2020, zuletzt geprüft am 06.10.2021.

Crowley, Michael; Glueck, Katie (2021): For Kamala Harris, an Influential Voice and a Decisive Vote. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2021/01/20/us/politics/kamala-harris-vice-president.html, zuletzt aktualisiert am 20.01.2021, zuletzt geprüft am 25.08.2021.

CSIS (2020): Significant Cyber Incidents. Hg. v. Center for Strategic and International Studies. Online verfügbar unter https://csis-prod.s3.amazonaws.com/s3fs-public/200108_Significant_Cyber_Events_List.pdf?aj4_VlDq2hSan2U8O5mS29Iurq3G1QKa.

Cyb3rsleuth (2013): Tracking Cybercrime. Hg. v. Cyb3rsleuth. Online verfügbar unter http://cyb3rsleuth.blogspot.com/search/label/Chinese%20Threats, zuletzt aktualisiert am 11.09.2013, zuletzt geprüft am 11.10.2021.

Cybereason (2022): About Dan Verton. Hg. v. Cybereason. Online verfügbar unter https://www.cybereason.com/blog/authors/dan-verton, zuletzt aktualisiert am 18.01.2022, zuletzt geprüft am 19.01.2022.

Cybereason Nocturnus (2021): Cybereason vs. DarkSide Ransomware. Hg. v. Cybereason. Online verfügbar unter https://www.cybereason.com/blog/cybereason-vs-darkside-ransomware, zuletzt aktualisiert am 01.04.2021, zuletzt geprüft am 02.01.2022.

da Conceição-Heldt, Eugénia; Mello, Patrick A. (2016): Two-Level Games in Foreign Policy Analysis. In: William R. Thompson (Hg.): Oxford research encyclopedias. Oxford.: Oxford University Press.

Daalder, Ivo H.; Lindsay, James M. (2003): America unbound: The Bush revolution in foreign policy: Brookings Institution Press.

Dahan, Michael (2013): Hacking for the Homeland: Patriotic Hackers versus Hacktivists. In: Douglas Hart (Hg.): CIW 2013 Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013. ICIW 2013 Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013: Academic Conferences Limited, S. 51–57, zuletzt geprüft am 15.05.2020.

Dark Reading (2017): FireEye Finds Russian Group APT28 Targeted Montenegro Government with Cyber Attacks. Hg. v. Dark Reading. Online verfügbar unter https://www.darkreading.com/threat-intelligence/fireeye-finds-russian-group-apt28-targeted-montenegro-government-with-cyber-attacks/d/d-id/1329060, zuletzt aktualisiert am 06.06.2017, zuletzt geprüft am 06.05.2021.

Dawisha, Karen (2015): Putin's kleptocracy: who owns Russia?: Simon and Schuster.

Debusmann, Bernd (2011): COLUMN – Goodbye to myth of Iran's ›mad mullahs‹? Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/usa-column-idINDEE7B80HN20111209, zuletzt aktualisiert am 09.12.2011, zuletzt geprüft am 03.01.2022.

Deibert, Ron (2015): Authoritarianism goes global: Cyberspace under siege. In: Journal of Democracy 26 (3), S. 64–78.

Deibert, Ronald J. (2009): The geopolitics of internet control: Censorship, sovereignty, and cyberspace. In: Routledge handbook of Internet politics, S. 323–336.

Delcour, Laure; Wolczuk, Kataryna (2015): Spoiler or facilitator of democratization?: Russia's role in Georgia and Ukraine. In: Democratization 22 (3), S. 459–478. DOI: 10.1080/13510347.2014.996135.

Demchak, Chris; Dombrowski, Peter (2013): Cyber Westphalia: Asserting state prerogatives in cyberspace. In: Georgetown Journal of International Affairs, S. 29–38.

Der Spiegel (2019): Benny Gantz: Hacker-Affäre torpediert Wahlkampf von Netanyahus ärgstem Widersacher. Hg. v. Der Spiegel. Online verfügbar unter https://www.spiegel.de/politik/ausland/israel-hacker-skandal-um-benjamin-netanyahus-gegner-benny-gantz-a-1258271.html, zuletzt aktualisiert am 17.03.2019, zuletzt geprüft am 05.01.2022.

Der Tagesspiegel (2021): Wegen Unterdrückung der Uiguren in Xinjiang: EU und USA verhängen Sanktionen gegen China – Vergeltung aus Peking folgt prompt. Hg. v. Der Tagesspiegel. Online verfügbar unter https://www.tagesspiegel.de/politik/wegen-unterdrueckung-der-uiguren-in-xinjiang-eu-und-usa-verhaengen-sankt

ionen-gegen-china-vergeltung-aus-peking-folgt-prompt/27027594.html, zuletzt aktualisiert am 22.03.2021, zuletzt geprüft am 27.07.2021.

Desai, Padma (2005): Russian retrospectives on reforms from Yeltsin to Putin. In: Journal of Economic Perspectives 19 (1), S. 87–106.

Deuber, Lea; Krüger, Paul-anton (2021): China und USA: Konfrontation um Taiwan. Hg. v. Süddeutsche Zeitung. Online verfügbar unter https://www.sueddeutsche.de/politik/china-usa-taiwan-militaeruebung-1.5187636, zuletzt aktualisiert am 28.01.2021, zuletzt geprüft am 30.07.2021.

Deutsche Welle (2008a): Chinas Kampf gegen die Uiguren. Hg. v. Deutsche Welle. Online verfügbar unter https://www.dw.com/de/chinas-kampf-gegen-die-uiguren/a-3245545, zuletzt aktualisiert am 11.04.2008, zuletzt geprüft am 27.07.2021.

Deutsche Welle (2008b): Medwedew nimmt Stellung zur Zukunft Russlands. Deutsche Welle (www.dw.com). Online verfügbar unter https://www.dw.com/de/medwedew-nimmt-stellung-zur-zukunft-russlands/a-3087458, zuletzt aktualisiert am 24.01.2008, zuletzt geprüft am 19.05.2021.

Deutsche Welle (2018): Niederlande vereiteln Cyber-Attacke russischer Spione auf OPCW. Deutsche Welle. Online verfügbar unter https://www.dw.com/de/niederlande-vereiteln-cyber-attacke-russischer-spione-auf-opcw/a-45751523, zuletzt aktualisiert am 04.10.2018, zuletzt geprüft am 12.05.2021.

Deutsche Welle (2020): Alexei Navalny dupes FSB agent into admitting role in poisoning. Deutsche Welle. Online verfügbar unter https://www.dw.com/en/alexei-navalny-dupes-fsb-agent-into-admitting-role-in-poisoning/a-56013446, zuletzt aktualisiert am 21.12.2020, zuletzt geprüft am 29.04.2021.

Deyermond, Ruth (2013): Assessing the reset: successes and failures in the Obama administration's Russia policy, 2009–2012. In: European Security 22 (4), S. 500–523. DOI: 10.1080/09662839.2013.777704.

Diamond, Jeremy (2016): Donald Trump: ›I'm afraid the election's going to be rigged‹ – CNNPolitics. Hg. v. CNN. Online verfügbar unter https://edition.cnn.com/2016/08/01/politics/donald-trump-election-2016-rigged/index.html, zuletzt aktualisiert am 03.08.2016, zuletzt geprüft am 27.09.2021.

Div, Lior (2018): Cybereason named Israel's most promising startup. Hg. v. Cyberreason. Online verfügbar unter https://www.cybereason.com/blog/calcalist-israel-most-proming-startup, zuletzt aktualisiert am 19.04.2018, zuletzt geprüft am 07.10.2021.

DoD (2020): Military and Security Developments involving the People's Republic of China 2020. Hg. v. Office of the Secretary of Defence (Annual Report to Congress). Online verfügbar unter https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF, zuletzt geprüft am 31.07.2021.

DoJ (2014a): U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor, zuletzt aktualisiert am 22.07.2015, zuletzt geprüft am 23.11.2020.

DoJ (2014b): U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage. Hg. v.

Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor, zuletzt aktualisiert am 22.07.2015, zuletzt geprüft am 29.07.2021.

DoJ (2017): U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions, zuletzt aktualisiert am 21.03.2017, zuletzt geprüft am 15.04.2021.

DoJ (2018a): Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal, zuletzt aktualisiert am 05.11.2018, zuletzt geprüft am 31.07.2021.

DoJ (2018b): Indictment against GRU Officers. Hg. v. Department of Justice. Online verfügbar unter https://int.nyt.com/data/documenthelper/80-netyksho-et-al-indictment/ba0521c1eef869deecbe/optimized/full.pdf?action=click&module=Intentional&pgtype=Article, zuletzt aktualisiert am 13.07.2018, zuletzt geprüft am 20.08.2021.

DoJ (2018c): Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion, zuletzt aktualisiert am 20.12.2018, zuletzt geprüft am 29.06.2021.

DoJ (2018d): U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and, zuletzt aktualisiert am 04.10.2018, zuletzt geprüft am 06.10.2021.

DoJ (2020a): Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking, zuletzt aktualisiert am 13.02.2020, zuletzt geprüft am 04.08.2021.

DoJ (2020b): Seven International Cyber Defendants, Including »Apt41« Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/press-release/file/1317206/download, zuletzt aktualisiert am 16.09.2021, zuletzt geprüft am 14.11.2021.

DoJ (2020c): Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace: Unsealed Indictment. Hg. v. US Department of Justice. Online verfügbar unter https://www.justice.gov/opa/press-release/file/1328521/download, zuletzt aktualisiert am 15.10.2020, zuletzt geprüft am 18.04.2021.

DoJ (2020d): Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Con-

fidential Business Information, Including COVID-19 Research. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/press-release/file/1295981/download, zuletzt aktualisiert am 22.07.2020, zuletzt geprüft am 01.07.2021.

DoJ (2021): Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research. Hg. v. Department of Justice. Online verfügbar unter https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion, zuletzt aktualisiert am 19.07.2021, zuletzt geprüft am 01.10.2021.

Dollar, David; Petri, Peter A. (2018): Why it's time to end the tit-for-tat tariffs in the U.S.-China trade war. Hg. v. Brookings. Online verfügbar unter https://www.brookings.edu/blog/order-from-chaos/2018/10/05/why-its-time-to-end-the-tit-for-tat-tariffs-in-the-u-s-china-trade-war/, zuletzt aktualisiert am 05.10.2018, zuletzt geprüft am 06.10.2021.

Dor, Ofir (2021): Palo Alto Networks founder Nir Zuk moves back to Israel. Hg. v. Globes. Online verfügbar unter https://en.globes.co.il/en/article-palo-alto-networks-founder-nir-zuk-moves-back-to-israel-1001364231, zuletzt aktualisiert am 16.03.2021, zuletzt geprüft am 11.10.2021.

Dorfman, Zach (2020a): China's Secret War for U.S. Data Blew American Spies' Cover. Hg. v. Foreign Policy. Online verfügbar unter https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/, zuletzt aktualisiert am 21.12.2020, zuletzt geprüft am 16.06.2021.

Dorfman, Zach (2020b): How China's Tech Giants Like Alibaba, Tencent, and Baidu Aid Spy Agencies. Hg. v. Foreign Policy. Online verfügbar unter https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/, zuletzt aktualisiert am 23.12.2020, zuletzt geprüft am 19.01.2022.

DoT (2018): Treasury Sanctions Russian Federal Security Service Enablers | U.S. Department of the Treasury. Hg. v. US Department of Treasury. Online verfügbar unter https://home.treasury.gov/news/press-releases/sm0410, zuletzt aktualisiert am 11.06.2018, zuletzt geprüft am 28.04.2021.

DoT (2019): Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware |. Hg. v. Department of the Treasury. Online verfügbar unter https://home.treasury.gov/news/press-releases/sm845, zuletzt aktualisiert am 05.12.2019, zuletzt geprüft am 15.04.2021.

DoT (2021): Treasury Sanctions Russia with Sweeping New Sanctions Authority. Hg. v. US Department of Treasury. Online verfügbar unter https://home.treasury.gov/news/press-releases/jy0127, zuletzt aktualisiert am 15.04.2021, zuletzt geprüft am 28.04.2021.

Doubek, James (2018): China Removes Presidential Term Limits, Enabling Xi Jinping To Rule Indefinitely. Hg. v. NPR. Online verfügbar unter https://www.npr.org/sections/thetwo-way/2018/03/11/592694991/china-removes-presidential-term-limits-enabling-xi-jinping-to-rule-indefinitely?t=1627206194175, zuletzt aktualisiert am 11.03.2018, zuletzt geprüft am 25.07.2021.

Duchâtel, Mathieu (2009): Hu Jintao and the People's Liberation Army. In: China Perspectives (3 (79)), S. 110–111. Online verfügbar unter http://www.jstor.org/stable/24054356.

Dudney, Robert S. (2011): Rise of the Cyber Militias. In: Air Force Magazine, S. 88–89.

Dumbrell, John (2018): The neoconservative roots of the war in Iraq. In: Intelligence and national security policymaking on Iraq: Manchester University Press, S. 19–39. Online verfügbar unter https://www.manchesterhive.com/view/9781526130969/9781526130969.00008.xml.

Easton, David (1975): A re-assessment of the concept of political support. In: British journal of political science 5 (4), S. 435–457.

ECPR (2017): China's »New Era« with Xi Jinping Characteristics. Hg. v. European Council on Foreign Relations (China Analysis). Online verfügbar unter https://ecfr.eu/wp-content/uploads/ECFR240_China_Analysis_Party_Congress_Ideology_2.pdf, zuletzt aktualisiert am 15.12.2017, zuletzt geprüft am 30.07.2021.

Egloff, Florian J. (2018): Cybersecurity and non-state actors: a historical analogy with mercantile companies, privateers, and pirates. University of Oxford. Online verfügbar unter https://ora.ox.ac.uk/objects/uuid:77eb9bad-ca00-48b3-abcf-d284c6d27571, zuletzt aktualisiert am 2018, zuletzt geprüft am 08.06.2020.

Egloff, Florian J. (2020a): Contested public attributions of cyber incidents and the role of academia. In: Contemporary Security Policy 41 (1), S. 55–81. DOI: 10.1080/13523260.2019.1677324.

Egloff, Florian J. (2020b): Public attribution of cyber intrusions. In: Journal of Cybersecurity 6 (1), Artikel tyaa012, S. 484. DOI: 10.1093/cybsec/tyaa012.

Egloff, Florian J.; Smeets, Max (2021): Publicly attributing cyber attacks: a framework. In: Journal of Strategic Studies, S. 1–32. DOI: 10.1080/01402390.2021.1895117.

Eichensehr, Kristen (2017): Public-private cybersecurity. In: Texas Law Review 95, S. 467–538.

Eichensehr, Kristen (2020): The Law & Politics of Cyberattack Attribution. In: UCLA Law Review 67.

Eichensehr, Kristen E. (2019): Decentralized Cyberattack Attribution. In: AJIL Unbound 113, S. 213–217. DOI: 10.1017/aju.2019.33.

Eiran, Ehud; Malin, Martin B. (2013): The Sum of all Fears: Israel's Perception of a Nuclear-Armed Iran. In: The Washington Quarterly 36 (3), S. 77–89.

Eoyang, Carson (1994): Models of Espionage. In: Theodore R. Sarbin, Ralph M. Carney und Carson Eoyang (Hg.): Citizen espionage. Studies in trust and betrayal. Westport, Conn.: Praeger, S. 69–92.

Epifanova, Alena (2020): Deciphering Russia's »Sovereign Internet Law«. Hg. v. DGAP. DGAP (DGAP Analysis, 2), zuletzt aktualisiert am 16.01.2020.

Erb, Guy; Sommers, Scott (2020): Still Losing Ground: The Consequences of the Trump Administration's Bilateral Trade Policy. Hg. v. Washington International Trade Association. Online verfügbar unter https://www.wita.org/blogs/losing-ground-trump-administrations-bilateral-trade/, zuletzt aktualisiert am 09.07.2020, zuletzt geprüft am 06.10.2021.

Ermert, Monika (2016): Last Formal Tie To Historic US Internet Control Is Cut – Intellectual Property Watch. Hg. v. Intellectual Property Watch. Online verfügbar

unter http://www.ip-watch.org/2016/10/01/last-formal-tie-to-historic-us-internet-control-is-cut/, zuletzt aktualisiert am 01.10.2016, zuletzt geprüft am 09.06.2021.
EURACTIV (2017): Merkel bekräftigt: »Ausspähen unter Freunden geht gar nicht«. Hg. v. EURACTIV. Online verfügbar unter https://www.euractiv.de/section/eu-innenpolitik/news/merkel-bekraeftigt-ausspaehen-unter-freunden-geht-gar-nicht/, zuletzt aktualisiert am 17.02.2017, zuletzt geprüft am 27.09.2021.
Fainberg, Sarah (2017): Russian Spetsnaz, contractors and volunteers in the Syrian conflict. In: IFRI Proliferation Papers (105), S. 1–27.
Farrell, Henry; Newman, Abraham L. (2019): Weaponized Interdependence: How Global Economic Networks Shape State Coercion. In: International Security 44 (1), S. 42–79. DOI: 10.1162/isec_a_00351.
Farwell, James P.; Rohozinski, Rafal (2011): Stuxnet and the future of cyber war. In: Survival 53 (1), S. 23–40.
Fearon, James D. (1995): Rationalist explanations for war. In: International Organization 49 (3), S. 379–414.
Feng, Chen (1998): Rebuilding the Party's Normative Authority: China's Socialist Spiritual Civilization Campaign. In: Problems of Post-Communism 45 (6), S. 33–41. DOI: 10.1080/10758216.1998.11655812.
Filippov, Gabor (2021): Hungary: Nations in Transit 2020 Country Report. Hg. v. Freedom House. Online verfügbar unter https://freedomhouse.org/country/hungary/nations-transit/2020, zuletzt aktualisiert am 26.04.2021, zuletzt geprüft am 26.04.2021.
Finch III, Raymond C. (2018): Vladimir Putin and the Russian Military. In: South Central Review 35 (1), S. 48–73.
Finkelstein, Norman H. (2005): Ariel Sharon. Minneapolis: Lerner Publications Company.
Finkle, Jim; Polityuk, Pavel (2018): U.S. seeks to take control of infected routers from hackers. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-cyber-routers-ukraine/cyber-firms-ukraine-warn-of-planned-russian-attack-idUSKCN1IO1U9, zuletzt aktualisiert am 23.05.2018, zuletzt geprüft am 19.04.2021.
Finnemore, Martha; Hollis, Duncan B. (2016): Constructing norms for global cybersecurity. In: American Journal of International Law 110 (3), S. 425–479.
Finnemore, Martha; Sikkink, Kathryn (1998): International norm dynamics and political change. In: International Organization, S. 887–917.
FireEye (2009): In-Q-Tel Invests in FireEye to Advance Cyber Security in the U.S. Intelligence Community. Hg. v. FireEye. Online verfügbar unter https://investors.fireeye.com/index.php/news-releases/news-release-details/q-tel-invests-fireeye-advance-cyber-security-us-intelligence, zuletzt aktualisiert am 18.11.2009, zuletzt geprüft am 12.08.2021.
FireEye (2014): APT28: A Window into Russia's Cyber Espionage Operations? | FireEye. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf, zuletzt geprüft am 19.04.2021.
FireEye (2015a): APT30 and the Mechanics. Of a Long-Running Cyber Espionage Operation. Online verfügbar unter https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf, zuletzt geprüft am 02.07.2021.

FireEye (2015b): Hiding in Plain Sight: FireEye and Microsoft Expose Chinese APT Group's Obfuscation Tactic | FireEye Inc. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/blog/threat-research/2015/05/hiding_in_plain_sigh.html, zuletzt aktualisiert am 14.05.2015, zuletzt geprüft am 25.06.2021.

FireEye (2016): Red Line Drawn: China Recalculates its Use of Cyber Espionage. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf, zuletzt geprüft am 04.08.2021.

FireEye (2017): APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat | FireEye Inc. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html, zuletzt aktualisiert am 06.04.2017, zuletzt geprüft am 25.05.2021.

Fish, M. Steven (2017): What Is Putinism? In: Journal of Democracy 28 (4), S. 61–75. DOI: 10.1353/jod.2017.0066.

Fisher, Max (2015): Did a Congressman just acknowledge the US took down North Korea's internet in December? Hg. v. Vox. Online verfügbar unter https://www.vox.com/2015/3/17/8235831/north-korea-internet-hack, zuletzt aktualisiert am 18.03.2015, zuletzt geprüft am 08.09.2021.

Flade, Florian; Mascolo, Georg (2021): Umstrittene Firma in Israel: BKA kaufte Spionagesoftware bei NSO. Hg. v. Tagesschau. Online verfügbar unter https://www.tagesschau.de/investigativ/ndr-wdr/spionagesoftware-nso-bka-101.html, zuletzt aktualisiert am 07.09.2021, zuletzt geprüft am 20.10.2021.

Floyd, Garry S. (2018): Attribution and Operational Art. Implications for Competing in Time. In: Strategic Studies Quarterly 12 (2), S. 17–55.

Ford, Matt (2019): The Trump Organization's Hostile Takeover of the U.S. Government | The New Republic. Hg. v. The New Republic. Online verfügbar unter https://newrepublic.com/article/155000/trump-organizations-hostile-takeover-us-government, zuletzt aktualisiert am 10.09.2021, zuletzt geprüft am 26.08.2021.

Frankenberg, Sydney (2020): Data-Driven Diplomacy: China's Growing Surveillance Industrial Complex | Stanford Rewired. Hg. v. Rewired (Issue One). Online verfügbar unter https://stanfordrewired.com/post/china-surveillance, zuletzt aktualisiert am 11.08.2020, zuletzt geprüft am 31.07.2021.

Fraser, Nalani; Plan, Fred; O'Leary Jacqueline; Cannon, Vincent; Leong, Raymond; Perez, Dan; Shen, Chi-en (2019): APT41: A Dual Espionage and Cyber Crime Operation. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html, zuletzt aktualisiert am 07.08.2019, zuletzt geprüft am 10.06.2021.

Fravel, M. Taylor (2015): China's New Military Strategy: ›Winning Informationized Local Wars‹. In: China Brief 15 (13), S. 3–7.

Freedman, Robert O. (2020a): Introduction to Israel in the Netanyahu era. In: Robert O. Freedman (Hg.): Israel Under Netanyahu: Domestic Politics and Foreign Policy: Routledge, S. 1–8.

Freedman, Robert O. (2020b): Israel and the United States: An uncertain Relationship. In: Robert O. Freedman (Hg.): Israel Under Netanyahu: Domestic Politics and Foreign Policy: Routledge, S. 135–160.

Freedom House (2019): Freedom in the World Countries. Hg. v. Freedom House. Online verfügbar unter https://freedomhouse.org/report/countries-world-freedom-2019.

F-Secure (2015): The Dukes. 7 Years of Russian Cyberespionage. Hg. v. F-Secure (Whitepaper). Online verfügbar unter https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf.

Fukuyama, Francis (2006): The end of history and the last man. New York: Simon and Schuster.

G Data (2014): Uroburos – hochkomplexe Spionagesoftware mit russischen Wurzeln. Hg. v. G Data (Red Paper). Online verfügbar unter https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf, zuletzt aktualisiert am Februar 2014, zuletzt geprüft am 14.04.2021.

Gady, Franz-Stefan (2015): New Snowden Documents Reveal Chinese Behind F-35 Hack. Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/, zuletzt aktualisiert am 27.01.2015, zuletzt geprüft am 25.05.2021.

Galeotti, Mark (2015): Putin's Spies and Security Men: His Strongest Allies, His Greatest Weakness. In: Stephen Aris, Matthias Neumann, Robert Orttung, Jeronim Perović, Heiko Pleines, Hans-Henning Schröder und Aglaya Snetkov (Hg.): Russia and Regime Security: ETH Zurich (RUSSIAN ANALYTICAL DIGEST, 173), S. 8–10.

Galeotti, Mark (2016a): Hybrid, ambiguous, and non-linear? How new is Russia's ›new way of war‹? In: Small wars & insurgencies 27 (2), S. 282–301.

Galeotti, Mark (2016b): Putin's hydra: inside Russia's intelligence services. Hg. v. European Council on Foreign Relations (Policy Brief). Online verfügbar unter https://ecfr.eu/archive/page/-/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf, zuletzt geprüft am 10.12.2021.

Galeotti, Mark (2017): Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe. European Council on Foreign Relations. Online verfügbar unter https://www.ecfr.eu/publications/summary/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe, zuletzt geprüft am 10.06.2020.

Galeotti, Mark (2019): The mythical ›Gerasimov Doctrine‹ and the language of threat. In: Critical Studies on Security 7 (2), S. 157–161. DOI: 10.1080/21624887.2018.1441623.

Gallagher, Sean (2018): Ukraine detects new Pterodo backdoor malware, warns of Russian cyberattack. Hg. v. Ars Technica. Online verfügbar unter https://arstechnica.com/information-technology/2018/11/ukraine-detects-new-pterado-backdoor-malware-warns-of-russian-cyberattack/, zuletzt aktualisiert am 20.11.2018, zuletzt geprüft am 01.01.2022.

Gareis, Sven Bernhard (2013): Taking off as a Global Power? China's Foreign Policy »Grand Strategy«. Hg. v. George C. Marshall European Center for Security Studies. Online verfügbar unter https://www.marshallcenter.org/en/publications/occasional-papers/taking-global-power-chinas-foreign-policy-grand-strategy, zuletzt aktualisiert am April 2013, zuletzt geprüft am 27.07.2021.

Gartzke, Erik (2000): Preferences and the democratic peace. In: International Studies Quarterly 44 (2), S. 191–212.

Gartzke, Erik (2013): The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. In: International Security 38 (2), S. 41–73. DOI: 10.1162/ISEC_a_00136.

Gechlik, Mei (2017): Appropriate Norms of State Behavior in Cyberspace: Governance in China and Opportunities for US Businesses. Hoover Institution (Aegis Series Paper, 1706).

Geddes, Barbara (1999): What Do We Know About Democratization After Twenty Years? In: Annual Review of Political Science 2 (1), S. 115–144. DOI: 10.1146/annurev.polisci.2.1.115.

Geddes, Barbara; Wright, Joseph; Frantz, Erica (2014): Autocratic breakdown and regime transitions: A new data set. In: Perspectives on Politics 12 (2), S. 313–331.

Geers, Kenneth; Kindlund, Darien; Moran, Ned; Rachwald, Rob (2014): World War C: Understanding nation-state motives behind today's advanced cyber attacks. In: FireEye, Milpitas, CA, USA, Tech. Rep., Sep.

Geller, Eric (2020): DHS cyber chief out after debunking Trump's election claims. Hg. v. Politico. Online verfügbar unter https://www.politico.com/news/2020/11/17/trump-fires-dhs-cybersecurity-chief-who-led-election-defense-437174, zuletzt aktualisiert am 18.11.2020, zuletzt geprüft am 06.10.2021.

Gel'man, Vladimir (2008): Party Politics in Russia: From Competition to Hierarchy. In: Europe-Asia Studies 60 (6), S. 913–930. DOI: 10.1080/09668130802161165.

George, Alexander L.; Bennett, Andrew (2005): The method of structured, focused comparison. In: Case studies and theory development in the social sciences, S. 67–73.

Georgieva, Ilina (2020): The unexpected norm-setters: Intelligence agencies in cyberspace. In: Contemporary Security Policy 41 (1), S. 33–54.

Gerschewski, Johannes (2013): The three pillars of stability: Legitimation, repression, and co-optation in autocratic regimes. In: Democratization 20 (1), S. 13–38.

Gertz, Bill (2014a): Chinese Military Creates High-Level Cyber Intelligence Center. Hg. v. The Washington Free Bacon. Online verfügbar unter https://freebeacon.com/national-security/chinese-military-creates-high-level-cyber-intelligence-center/, zuletzt aktualisiert am 03.07.2014, zuletzt geprüft am 07.07.2021.

Gertz, Bill (2014b): New Chinese Intelligence Unit Linked to Massive Cyber Spying Program. Hg. v. The Washington Free Beacon. Online verfügbar unter https://freebeacon.com/national-security/new-chinese-intelligence-unit-linked-to-massive-cyber-spying-program/, zuletzt aktualisiert am 31.10.2014, zuletzt geprüft am 01.07.2021.

Gertz, Bill (2015): FBI Alert Reveals ›Groups‹ Behind OPM Hack. Hg. v. The Washington Free Bacon. Online verfügbar unter https://freebeacon.com/national-security/fbi-alert-reveals-groups-behind-opm-hack/, zuletzt aktualisiert am 10.06.2015, zuletzt geprüft am 12.11.2021.

Gertz, Bill (2016a): Chinese Military Revamps Cyber Warfare, Intelligence Forces. Hg. v. The Washington Free Beacon. Online verfügbar unter https://freebeacon.com/national-security/chinese-military-revamps-cyber-warfare-intelligence-forces/, zuletzt aktualisiert am 27.01.2016, zuletzt geprüft am 07.07.2021.

Gertz, Bill (2016b): Pentagon Links Chinese Cyber Security Firm to Beijing Spy Service. Hg. v. The Washington Free Beacon. Online verfügbar unter https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/, zuletzt aktualisiert am 29.11.2016, zuletzt geprüft am 29.06.2021.

Gierow, Hauke (2018): Chinese hackers are expected to put their country first. Hg. v. Merics. Online verfügbar unter https://merics.org/de/analyse/chinese-hackers-are-expected-put-their-country-first, zuletzt aktualisiert am 18.04.2018, zuletzt geprüft am 11.10.2021.

Gilens, Martin; Page, Benjamin I. (2014): Testing theories of American politics: Elites, interest groups, and average citizens. In: Perspectives on Politics 12 (3), S. 564–581.

Giles, Keir (2011): »Information Troops«-A Russian Cyber Command? In: Christian Czosseck, E. Tyugu und T. Wingfield (Hg.): 2011 3rd International Conference on Cyber Conflict. Tallinn, Estonia: CCD COE Publications, S. 45–60.

Giles, Keir (2012): Russia's public stance on cyberspace issues. 4th International Conference on Cyber Conflict (CYCON 2012). Tallinn.

Gilli, Andrea; Gilli, Mauro (2019): Why China has not caught up yet: military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage. In: International Security 43 (3), S. 141–189.

Gleicher, Nathaniel (2020): Taking Action Against Hackers in Bangladesh and Vietnam. Hg. v. Meta. Online verfügbar unter https://about.fb.com/news/2020/12/taking-action-against-hackers-in-bangladesh-and-vietnam/amp/, zuletzt aktualisiert am 11.12.2020, zuletzt geprüft am 11.01.2022.

Göbel, Christian (2015): Why does China Have Internet? Contagion, contingency and strategy in China's ICT management. Hg. v. Christian Göbel. Wien. Online verfügbar unter https://christiangoebel.net/why-does-china-have-internet-contagion-contingency-and-strategy-in-chinas-ict-management-2, zuletzt aktualisiert am 20.10.2015.

Göbel, Christian; Ong, Lynette H. (2012): Social unrest in China. Hg. v. Europe China Research and Advice Network. London. Online verfügbar unter https://d1wqtxts1xzle7.cloudfront.net/34690494/ECRAN_Social_Unrest_in_China__Christian_Gobel_and_Lynette_H._Ong-with-cover-page-v2.pdf?Expires=1627399212&Signature=XDKNZJrXDpR4GA5ITZBDMTizVlMBiiUixQYEyx6pScBf9n~GT-X-BTv0q2MNX2AraAQCFn5ZlvjTrCAg4Jumq4jF30D-q9W4m8TbPvqwf43OFIIW0Jnflxw~3WwThoetuOCA0SL8sx3l~pc0z5PSmkmKhnGae2cBLtu4TYuJ1ZR2E9eRmBnhX7FBPJda8iIWFXA6smAEM-NZL9IVNAH6LC8f92lIGvLVT0KgqaVFxpkyEDsvu8Y7lLUn8dmf~0HMDpKHFeOSqFPy8HappPsk6a40bZZzZwvsiiRpwVit6~ylmZ~1auH3u5AQSC570bKOhdaynLExY3wSvqn27nkZOA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA, zuletzt geprüft am 27.07.2021.

Goertz, Gary (2012): Social science concepts: A user's guide. Princeton, Oxford: Princeton University Press.

Goldberg, Giora (2006): The Growing Militarization of the Israeli Political System. In: Israel Affairs 12 (3), S. 377–394. DOI: 10.1080/13537120600744594.

Goldstein, Judith; Keohane, Robert O. (1993): Ideas and foreign policy: beliefs, institutions, and political change: Cornell University Press.

Gorwa, Robert; Smeets, Max (2019): Cyber Conflict in Political Science: A Review of Methods and Literature (Working Paper Prepared for the 2019 ISA Annual Convention). Online verfügbar unter https://osf.io/preprints/socarxiv/fc6sg/, zuletzt geprüft am 05.08.2021.

Goulard, Sebastien (2020): The Impact of the US–China Trade War on the European Union. In: Global Journal of Emerging Market Economies 12 (1), S. 56–68. DOI: 10.1177/0974910119896642.

Gould-Davies, Nigel (2016): Russia's Sovereign Globalization: Rise, Fall and Future. Hg. v. Chatham House. Online verfügbar unter https://www.chathamhouse.org/2016/01/russias-sovereign-globalization-rise-fall-and-future, zuletzt aktualisiert am 06.01.2016, zuletzt geprüft am 05.05.2021.

Gov.UK (2018): Joint statement from Prime Minister May and Prime Minister Rutte. Hg. v. Government UK. Online verfügbar unter https://www.gov.uk/government/news/joint-statement-from-prime-minister-may-and-prime-minister-rutte, zuletzt aktualisiert am 04.10.2018, zuletzt geprüft am 06.10.2021.

Government of Canada (2018): Canada identifies malicious cyber-activity by Russia. Hg. v. Government of Canada. Online verfügbar unter https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html, zuletzt aktualisiert am 04.10.2018, zuletzt geprüft am 06.10.2021.

Gowan, Richard (2020): China's pragmatic approach to UN peacekeeping. Hg. v. Brookings. Online verfügbar unter https://www.brookings.edu/articles/chinas-pragmatic-approach-to-un-peacekeeping/, zuletzt aktualisiert am 14.09.2020, zuletzt geprüft am 30.07.2021.

Graff, Garrett M. (2018): Robert Mueller's Indictment Today of 12 Russian Hackers Could Be His Biggest Move Yet. Hg. v. Wired. Online verfügbar unter https://www.wired.com/story/mueller-indictment-dnc-hack-russia-fancy-bear/, zuletzt aktualisiert am 13.07.2018, zuletzt geprüft am 19.04.2021.

Graham, Alex (2019): State of the Venture Capital Industry in 2019 (with Infographic). Hg. v. Toptal. Online verfügbar unter https://www.toptal.com/finance/venture-capital-consultants/state-of-venture-capital-industry-2019, zuletzt aktualisiert am 20.06.2019, zuletzt geprüft am 26.10.2021.

Grant, Charles (2012): Russia, China and global governance. London: Centre for European Reform.

Grauvogel, Julia; Soest, Christian von (2014): Claims to legitimacy count: Why sanctions fail to instigate democratisation in authoritarian regimes. In: Eur J Polit Res 53 (4), S. 635–653. DOI: 10.1111/1475-6765.12065.

Green, James A. (Hg.) (2016): Cyber warfare. A multidisciplinary analysis. London: Routledge, Taylor & Francis Group (Routledge studies in conflict, security and technology, 2016: 1).

Greenberg, Andy (2018): The untold story of NotPetya, the most devastating cyberattack in history. Hg. v. Wired. Online verfügbar unter https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, zuletzt aktualisiert am 22.08.2018.

Greenberg, Andy (2019a): Russia's ›Sandworm‹ Hackers Also Targeted Android Phones. Hg. v. Wired. Online verfügbar unter https://www.wired.com/story/sandworm-android-malware/, zuletzt aktualisiert am 21.11.2019, zuletzt geprüft am 10.06.2021.

Greenberg, Andy (2019b): Sandworm. A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. First edition. New York: Doubleday.

Greene, Abner S. (1994): Checks and Balances in an Era of Presidential Lawmaking. In: The University of Chicago Law Review 61 (1), S. 123. DOI: 10.2307/1600091.

Grey Goose (2009): Project Grey Goose Phase II Report: The evolving state of cyber warfare. Hg. v. GreyLogic. Online verfügbar unter https://www.nytimes.com/1992/03/08/world/us-strategy-plan-calls-for-insuring-no-rivals-develop.html, zuletzt aktualisiert am 20.03.2009, zuletzt geprüft am 26.08.2021.

Griffith, Melissa K. (2018): Why Cyber Conflict as an Academic Discipline Struggles to Make Its Mark in Political Sciene. Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/blog/why-cyber-conflict-academic-discipline-struggles-make-its-mark-political-science, zuletzt aktualisiert am 06.09.2018.

Groll, Elias (2016): New Evidence Strengthens Guccifer 2.0's Russian Connections. Hg. v. Foreign Policy. Online verfügbar unter https://foreignpolicy.com/2016/07/26/new-evidence-strengthens-guccifer-2-0s-russian-connections/, zuletzt aktualisiert am 26.07.2016, zuletzt geprüft am 20.08.2021.

Gschwend, Thomas; Schimmelfennig, Frank (2007): Forschungsdesign in der Politikwissenschaft: ein Dialog zwischen Theorie und Daten 11. Online verfügbar unter https://www.ssoar.info/ssoar/handle/document/25827.

Guarnieri, Claudio (2015): Digitaler Angriff auf den Bundestag: Investigativer Bericht zum Hack der IT-Infrastruktur der Linksfraktion. Hg. v. netzpolitik.org. Online verfügbar unter https://netzpolitik.org/2015/digitaler-angriff-auf-den-bundestag-investigativer-bericht-zum-hack-der-it-infrastruktur-der-linksfraktion/, zuletzt aktualisiert am 10.07.2018, zuletzt geprüft am 19.04.2021.

Gueorguiev, Dimitar; Shao, Li; Crabtree, Charles (2018): Blurring the Lines: Rethinking Self-Censorship under Autocracy. Online verfügbar unter https://www.researchgate.net/profile/Dimitar_Gueorguiev2/publication/321636833_Blurring_the_Lines_Rethinking_Censorship_Under_Autocracy/links/5b418be0458515f71cb11ffb/Blurring-the-Lines-Rethinking-Censorship-Under-Autocracy.pdf, zuletzt aktualisiert am 09.05.2018.

Guerrero-Saade, Juan Andres; Raiu, Costin (2017): Walking in your enemy's shadow: when fourth-party collection becomes attribution hell. Virus Bulletin Conference. Virus Bulletin, 2017. Online verfügbar unter https://www.virusbulletin.com/uploads/pdf/magazine/2017/VB2017-Guerrero-Saade-Raiu.pdf.

Guitton, Clement; Korzak, Elaine (2013): The Sophistication Criterion for Attribution. In: The RUSI Journal 158 (4), S. 62–68. DOI: 10.1080/03071847.2013.826509.

Gunitsky, Seva (2015): Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability. Perspectives on Politics, 13(1), 42–54. DOI: 10.1017/S1537592714003120.

Haas, Ernst B. (1980): Why collaborate? Issue-linkage and international regimes. In: World politics 32 (3), S. 357–405.

Haberman, Maggie; Martin, Jonathan (2021): After the Speech: What Trump Did as the Capitol Was Attacked. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2021/02/13/us/politics/trump-capitol-riot.html?, zuletzt aktualisiert am 13.02.2021, zuletzt geprüft am 26.08.2021.

Hacker, Jacob S.; Pierson, Paul (2010): Winner-take-all politics: How Washington made the rich richer–and turned its back on the middle class: Simon and Schuster.

Hacquebord, Feike; Remorin, Alfred (2020): Pawn Storm's Lack of Sophistication as a Strategy. Hg. v. Trend Micro. Online verfügbar unter https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html, zuletzt aktualisiert am 17.12.2020, zuletzt geprüft am 20.04.2021.

Haizler, Omry (2017): The United States' cyber warfare history: Implications on modern cyber operational structures and policymaking. In: Cyber, Intelligence, and Security 1 (1), S. 31–45.

Halchin, Elaine (2015): The Intelligence Community and Its Use of Contractors: Congressional Oversight Issues. Hg. v. Congressional Research Service. Online verfügbar unter https://sgp.fas.org/crs/intel/R44157.pdf, zuletzt aktualisiert am 18.08.2015, zuletzt geprüft am 27.09.2021.

Hale, Henry E. (2011): The Myth of Mass Russian Support for Autocracy: The Public Opinion Foundations of a Hybrid Regime. In: Europe-Asia Studies 63 (8), S. 1357–1375. DOI: 10.1080/09668136.2011.601106.

Hall, Peter A. (2003): Aligning Ontology and Methodology in Comparative Research. In: James Mahoney und Dietrich Rueschemeyer (Hg.): Comparative Historical Analysis in the Social Sciences. Cambridge, UK and New York: Cambridge University Press, 373–404.

Hanna, Andrew (2019): The Invisible U.S.-Iran Cyber War. Hg. v. United States Institute of Peace. Online verfügbar unter https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war, zuletzt aktualisiert am 25.10.2019, zuletzt geprüft am 06.10.2021.

Hansel, Mischa; Mutschler, Max; Dickow, Marcel (2018): Taming cyber warfare: lessons from preventive arms control. In: Journal of Cyber Policy 3 (1), S. 44–60. DOI: 10.1080/23738871.2018.1462394.

Hansel, Mischa; Nanni, Sara (2018): Quantitative Rüstungsanalysen im Zeichen von Digitalisierung und Automatisierung. In: ZIB Zeitschrift für Internationale Beziehungen 25 (1), S. 211–220. DOI: 10.5771/0946-7165-2018-1-211.

Harding, Luke (2007): Putin, the Kremlin power struggle and the $40bn fortune. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2007/dec/21/russia.topstories3, zuletzt aktualisiert am 21.12.2007, zuletzt geprüft am 12.05.2021.

Harding, Luke; Borger, Julian; Sabbagh, Dan (2021): Kremlin papers appear to show Putin's plot to put Trump in White House. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2021/jul/15/kremlin-papers-appear-to-show-putins-plot-to-put-trump-in-white-house, zuletzt aktualisiert am 15.07.2021, zuletzt geprüft am 29.07.2021.

Harel, Amos; Levinson, Chaim (2021): After NSO blacklisting, Israel fears U.S. targeting all Israeli offensive cyber firms. Hg. v. Haaretz. Online verfügbar unter https://www.haaretz.com/israel-news/not-just-nso-israel-fears-u-s-targeting-all-israeli-offensive-cyber-firms-1.10463087, zuletzt aktualisiert am 14.12.2021, zuletzt geprüft am 03.01.2022.

Harel, Amos; Levinson, Chaim; Kubovich, Yaniv (2021): Israeli authorities inspect NSO Group offices after Pegasus revelations. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/news/2021/jul/29/israeli-authorities-inspect-

nso-group-offices-after-pegasus-revelations, zuletzt aktualisiert am 29.07.2021, zuletzt geprüft am 03.01.2022.

Harnisch, Sebastian (2018): Deutschlands Politik gegenüber der Belt-and-Road-Initiative der Volksrepublik China 2013–2018. In: ASIEN: The German Journal on Contemporary Asia (148), S. 26–50.

Harnisch, Sebastian (2021): Spreading Cyber-Autocracy? The Shanghai Cooperation Organization and the Diffusion of Norms of »Internet Sovereignty«. In: Marianne Kneuer und Thomas Demmelhuber (Hg.): Authoritarian gravity centers. A cross-regional study of authoritarian promotion and diffusion. New York, London: Routledge (Conceptualising comparative politics, 11), S. 249–274.

Harnisch, Sebastian; Friedrichs, Gordon (2017): Alliances Rebalanced? The Social Meaning of the US Pivot and Allies' Responses in Northeast Asia. In: The Korean Journal of International Studies 15 (1), S. 1–39.

Harnisch, Sebastian; Zettl, Kerstin; Steiger, Stefan (2021): Heidelberg Cyber Conflict Dataset (HD-CY.CON). Unter Mitarbeit von Sebastian Harnisch. Hg. v. Institut für Politische Wissenschaft, Universität Heidelberg. Online verfügbar unter https://heidata.uni-heidelberg.de/dataset.xhtml?persistentId=doi:10.11588/data/KDSFRB, zuletzt aktualisiert am 2021, zuletzt geprüft am 27.12.2021.

Harris, Shane (2008): China's cyber-militia. In: National Journal Magazine 31.

Harrison, Virginia; Palumbo, Daniele (2019): China anniversary: How the country became the world's ›economic miracle‹. Hg. v. BBC. Online verfügbar unter https://www.bbc.com/news/business-49806247, zuletzt aktualisiert am 01.10.2019, zuletzt geprüft am 25.07.2021.

Healey, Jason (2011): The Spectrum of National Responsibility for Cyberattacks. In: The Brown Journal of World Affairs 18 (1), S. 57–70. Online verfügbar unter http://www.jstor.org/stable/24590776.

Healey, Jason (2018): The State of the Field of Cyber Conflict. Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/blog/state-field-cyber-conflict, zuletzt aktualisiert am 12.11.2018.

Healey, Jason; Jervis, Robert (2020): The Escalation Inversion and Other Oddities of Situational Cyber Stability. In: Texas National Security Review 3 (4).

Healey, Jason; Piiparinen, Anni (2015): Did China Just Hack the International Court Adjudicating Its South China Sea Territorial Claims? Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2015/10/did-china-just-hack-the-international-court-adjudicating-its-south-china-sea-territorial-claims/, zuletzt aktualisiert am 27.10.2015, zuletzt geprüft am 23.06.2021.

Healey, Jason; Wilson, A. J. (2012): Cyber Conflict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain. In: Georgetown Journal of International Affairs, S. 59–69. Online verfügbar unter http://www.jstor.org/stable/43134339.

Hefele, Peter; Merkle, David; Zhivkov, Sasha (2015): Mit Konfuzius nach Afrika. Wie Auswärtige Kulturpolitik Chinas Simme und Sicht der Welt vermitteln soll. Hg. v. Konrad-Adenauer-Stiftung (KAS Auslandsinformationen, 05/2015). Online verfügbar unter https://www.kas.de/c/document_library/get_file?uuid=789580c9-5ef9-4e63-5731-038d86272d10&groupId=252038, zuletzt geprüft am 27.07.2021.

Hegel, Tom (2018): Burning Umbrella. An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers. Hg. v. ProtectWise 401TRG.

Heilmann, Sebastian (2018): Charakteristika des politischen Systems. Hg. v. Bundeszentrale für Politische Bildung (Dossier China). Online verfügbar unter https://www.bpb.de/internationales/asien/china/44270/charakteristika-des-politischen-systems, zuletzt aktualisiert am 07.09.2018, zuletzt geprüft am 09.07.2021.

Henriksen, Anders (2019): The end of the road for the UN GGE process: The future regulation of cyberspace. In: Journal of Cybersecurity 5 (1). DOI: 10.1093/cybsec/tyy009.

Henry, Laura A.; Sundstrom, Lisa McIntosh (2012): Russia's Climate Policy: International Bargaining and Domestic Modernisation. In: Europe-Asia Studies 64 (7), S. 1297–1322. DOI: 10.1080/09668136.2012.701388.

Herd, Graeme P. (2019): Putin's Operational Code and Strategic Decision-Making in Russia. In: Roger E. Kanet (Hg.): Routledge Handbook of Russian Security. Milton: Routledge, S. 17–29.

Herpig, Sven; Morgus, Robert; Sheniak, Amit (2020): Active Cyber Defense- A comparative study on US, Israeli and German approaches. Hg. v. Konrad-Adenauer-Stiftung. Online verfügbar unter https://www.kas.de/documents/263458/263507/Active+Cyber+Defense+-+A+comparative+study+on+US,+Israeli+and+German+approaches.pdf, zuletzt geprüft am 06.01.2022.

HIIK (2016): Conflict Barometer 2016. Hg. v. Heidelberger Institut für internationale Konfliktforschung. Heidelberg. Online verfügbar unter http://hiik.de/de/konfliktbarometer/pdf/ConflictBarometer_2016.pdf, zuletzt geprüft am 20.12.2020.

Hill, Fiona (2021): The Kremlin's Strange Victory: How Putin Exploits American Dysfunction and Fuels American Decline. Hg. v. Foreign Affairs. Online verfügbar unter https://www.foreignaffairs.com/articles/united-states/2021-09-27/kremlins-strange-victory?utm_medium=promo_email&utm_source=lo_flows&utm_campaign=registered_user_welcome&utm_term=email_1&utm_content=20211006, zuletzt aktualisiert am 27.09.2021, zuletzt geprüft am 06.10.2021.

Hjortdal, Magnus (2011): China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. In: JSS 4 (2), S. 1–24. DOI: 10.5038/1944-0472.4.2.1.

Hoang, Viet (2020): The Code of Conduct for the South China Sea: A Long and Bumpy Road. Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2020/09/the-code-of-conduct-for-the-south-china-sea-a-long-and-bumpy-road/, zuletzt aktualisiert am 28.09.2020, zuletzt geprüft am 02.08.2021.

Hoffman, Ronen (2019): Israel's foreign policy under Benjamin Netanyahu. In: Foreign Policy Research Institute 18.

Hoffman, Samantha; Mattis, Peter (2016): Managing the Power Within: China's State Security Commission. Hg. v. War on the Rocks. Online verfügbar unter https://warontherocks.com/2016/07/managing-the-power-within-chinas-state-security-commission/, zuletzt aktualisiert am 20.07.2016, zuletzt geprüft am 16.06.2021.

Holbig, Heike (2009): Remaking the CCP's Ideology: Determinants, Progress, and Limits under Hu Jintao. In: Journal of Current Chinese Affairs 38 (3), S. 35–61.

Holbig, Heike; Gilley, Bruce (2010): Reclaiming legitimacy in China. In: Politics & policy 38 (3), S. 395–422.

Holbig, Heike; Mittelstaedt, Jean Christopher; Sautin, Yevgen; Stanzel, Angela (2017): China's »New Era« with Xi Jinping characteristics. Hg. v. European Council on Foreign Relations. Online verfügbar unter https://ecfr.eu/wp-content/uploads/ECFR240_China_Analysis_Party_Congress_Ideology_2.pdf, zuletzt aktualisiert am 15.12.2017, zuletzt geprüft am 10.02.2022.

Holt, Alexander (2020): A brief history of US-China espionage entanglements. Hg. v. MIT Technology Review. Online verfügbar unter https://www.technologyreview.com/2020/09/03/1007609/trade-secrets-china-us-espionage-timeline/, zuletzt aktualisiert am 03.09.2020, zuletzt geprüft am 27.07.2021.

Homolar, Alexandra (2011): Rebels without a conscience: The evolution of the rogue states narrative in US security policy. In: European Journal of International Relations 17 (4), S. 705–727. DOI: 10.1177/1354066110383996.

Horchert, Judith (2017): Kaspersky-Chef: »Wir schützen unsere Kunden vor Malware – sei sie nun russisch oder amerikanisch«. Hg. v. Der Spiegel. Online verfügbar unter https://www.spiegel.de/netzwelt/netzpolitik/kaspersky-firmenchef-eugene-kaspersky-verteidigt-sich-gegen-anschuldigungen-a-1167916.html, zuletzt aktualisiert am 16.09.2017, zuletzt geprüft am 21.03.2020.

Hovet, Jason (2018): Czech security service says Russia behind cyber attacks on ministry. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-czech-security-russia-idUSKBN1O21BN, zuletzt aktualisiert am 03.12.2018, zuletzt geprüft am 14.04.2021.

Hsiao, Russell (2010): China's Cyber Command? Hg. v. Jamestown Foundation. Online verfügbar unter https://jamestown.org/program/chinas-cyber-command/, zuletzt aktualisiert am 18.09.2016, zuletzt geprüft am 05.07.2021.

Hsu, Kimberly; Murray, Craig; Wild, Matt (2013): China's 2012 Defense White Paper: The Diversified Employment of China's Armed Forces. Hg. v. U.S.-China Economic and Security Review Commission Staff Research Backgrounder. Online verfügbar unter https://www.uscc.gov/sites/default/files/Research/China%E2%80%99s%202012%20Defense%20White%20Paper--The%20Diversified%20Employment%20of%20China%E2%80%99s%20Armed%20Forces.pdf, zuletzt geprüft am 05.07.2021.

Huetteman, Emmarie (2017): Obama White House Knew of Russian Election Hacking, but Delayed Telling. Hg. v. The Straits Times. Online verfügbar unter https://www.nytimes.com/2017/06/21/us/politics/jeh-johnson-testimony-russian-election-hacking.html, zuletzt aktualisiert am 21.06.2017, zuletzt geprüft am 08.09.2021.

Hulcoop, Adam; Scott-Railton, John; Tanchak, Peter; Brooks, Matt; Deibert, Ron (2017): Tainted leaks: Disinformation and phishing with a Russian nexus. University of Toronto (Citizen Lab Research Report, 92).

Human Rights Watch (2007): World Report 2007. Hg. v. Human Rights Watch. Online verfügbar unter https://www.hrw.org/sites/default/files/reports/wr2007master.pdf, zuletzt geprüft am 27.07.2021.

Hummel, Philipp (2017): Wie kann die Politik Hackerangriffen entgehen? Hg. v. Spektrum. Online verfügbar unter https://www.spektrum.de/news/stecken-russische-hacker-hinter-den-angriffen-auf-politiker/1485839, zuletzt aktualisiert am 27.07.2017, zuletzt geprüft am 05.05.2021.

Hunnicutt, Trevor (2021): Biden orders probe of latest ransomware attack. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/technology/biden-says-uncertain-who-is-behind-latest-ransomware-attack-2021-07-03/, zuletzt aktualisiert am 04.07.2021, zuletzt geprüft am 05.07.2021.

Iasiello, Emilio (2016): China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities. In: JSS 9 (2), S. 45–69. Online verfügbar unter http://www.jstor.org/stable/26466776.

IISS (2021a): Cyber Power – Tier One. Hg. v. International Institute for Strategic Studies. Online verfügbar unter https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-one, zuletzt aktualisiert am 28.06.2021, zuletzt geprüft am 24.08.2021.

IISS (2021b): Cyber Power – Tier Two. Russia. Hg. v. International Institute for Strategic Studies. Online verfügbar unter https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-two, zuletzt aktualisiert am 28.06.2021, zuletzt geprüft am 04.08.2021.

IISS (2021c): Cyber Power – Tier Two: Israel. Hg. v. International Institute for Strategic Studies. Online verfügbar unter https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-two, zuletzt aktualisiert am 28.06.2021, zuletzt geprüft am 25.10.2021.

Ilievski, Aleksandar; Bernik, Igor (2016): Social-economic aspects of cybercrime. In: Peer-reviewed academic journal Innovative Issues and Approaches in Social Sciences 9 (3), S. 8–22.

Inbar, Efraim (2020): Israel's pivot from Europe to Asia. In: Robert O. Freedman (Hg.): Israel Under Netanyahu: Domestic Politics and Foreign Policy: Routledge, S. 242–261.

Insikt Group (2017a): North Korea's ruling elite are not isolated. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/north-korea-internet-activity/, zuletzt aktualisiert am 25.07.2017, zuletzt geprüft am 08.06.2020.

Insikt Group (2017b): Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/chinese-mss-behind-apt3/, zuletzt aktualisiert am 03.03.2021, zuletzt geprüft am 01.07.2021.

Insikt Group (2018a): Chinese Threat Actor TEMP.Periscope Targets UK-Based Engineering Company Using Russian APT Techniques. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/chinese-threat-actor-tempperiscope/, zuletzt aktualisiert am 13.01.2021, zuletzt geprüft am 01.07.2021.

Insikt Group (2018b): RedAlpha: New Campaigns Discovered Targeting the Tibetan Community. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/redalpha-cyber-campaigns/, zuletzt aktualisiert am 26.06.2018, zuletzt geprüft am 25.06.2021.

Insikt Group (2021a): China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/redecho-targeting-indian-power-sector/, zuletzt aktualisiert am 17.06.2021, zuletzt geprüft am 04.08.2021.

Insikt Group (2021b): China's PLA Unit is Purchasing Foreign Antivirus Products. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/china-p

la-unit-purchasing-antivirus-exploitation/, zuletzt aktualisiert am 05.05.2021, zuletzt geprüft am 05.07.2021.

Insikt Group (2021c): Chinese State-Sponsored Activity Group TAG-22 Targets Nepal, the Philippines, and Taiwan Using Winnti and Other Tooling. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/, zuletzt aktualisiert am 28.07.2021, zuletzt geprüft am 14.11.2021.

Insikt Group (2021d): Threat Activity Group RedFoxtrot Targets Bordering Asian Countries. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/redfoxtrot-china-pla-targets-bordering-asian-countries/?__hstc=156209188.afd5a56f082997c45b3ad6c0258a1b38.1625493199219.1625493199219.1625493199219.1&__hssc=156209188.1.1625493199219&__hsfp=1762131360, zuletzt aktualisiert am 17.06.2021, zuletzt geprüft am 05.07.2021.

Interfax (2015): Putin's electoral rating reaches new high in late March. Hg. v. Russia Beyond. Online verfügbar unter https://www.rbth.com/news/2015/03/27/putins_electoral_rating_reaches_new_high_in_late_march_44819.html, zuletzt aktualisiert am 27.03.2015, zuletzt geprüft am 10.06.2021.

Interfax (2017): В Минобороны РФ создали войска информационных операций [Im RF-Verteidigungsministerium wurden Truppen für Informationsoperationen eingesetzt]. Hg. v. Interfax.ru. Online verfügbar unter https://www.interfax.ru/russia/551054, zuletzt aktualisiert am 22.02.2017, zuletzt geprüft am 27.04.2021.

Intrusion Truth (2017): APT3 is Boyusec, a Chinese Intelligence Contractor. Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/, zuletzt aktualisiert am 10.05.2017, zuletzt geprüft am 29.06.2021.

Intrusion Truth (2018a): APT10 was managed by the Tianjin bureau of the Chinese Ministry of State Security. Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2018/08/15/apt10-was-managed-by-the-tianjin-bureau-of-the-chinese-ministry-of-state-security/, zuletzt aktualisiert am 15.08.2018, zuletzt geprüft am 29.06.2021.

Intrusion Truth (2018b): The destruction of APT3. Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2018/05/22/the-destruction-of-apt3/, zuletzt aktualisiert am 22.05.2018, zuletzt geprüft am 29.06.2021.

Intrusion Truth (2019a): APT17 is run by the Jinan bureau of the Chinese Ministry of State Security. Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2019/07/24/apt17-is-run-by-the-jinan-bureau-of-the-chinese-ministry-of-state-security/, zuletzt aktualisiert am 09.07.2019, zuletzt geprüft am 29.06.2021.

Intrusion Truth (2019b): Encore! APT17 hacked Chinese targets and offered the data for sale. Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2019/07/25/encore-apt17-hacked-chinese-targets-and-offered-the-data-for-sale/, zuletzt aktualisiert am 24.07.2019, zuletzt geprüft am 29.06.2021.

Intrusion Truth (2019c): Who is Mr Guo? Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2019/07/17/who-is-mr-guo/, zuletzt aktualisiert am 11.07.2019, zuletzt geprüft am 29.06.2021.

Intrusion Truth (2020): APT40 is run by the Hainan department of the Chinese Ministry of State Security. Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2020/01/16/apt40-is-run-by-the-hainan-department-of-the-chinese-ministry-of-state-security/, zuletzt aktualisiert am 16.01.2020, zuletzt geprüft am 30.06.2021.

Intrusion Truth (2021): An APT with no name. Hg. v. Intrusion Truth. Online verfügbar unter https://intrusiontruth.wordpress.com/2021/05/06/an-apt-with-no-name/, zuletzt aktualisiert am 06.05.2021, zuletzt geprüft am 20.01.2022.

Ip, Greg (2020): Checks and Balances Erode as Trump Flexes Power of the Purse. Hg. v. The Wall Street Journal. Online verfügbar unter https://www.wsj.com/articles/checks-and-balances-erode-as-trump-flexes-power-of-the-purse-11597237218, zuletzt aktualisiert am 12.08.2020, zuletzt geprüft am 26.08.2021.

IT Times (2020): Microsoft schluckt israelisches Cybersecurity-Startup CyberX. Hg. v. IT Times. Online verfügbar unter https://www.it-times.de/news/microsoft-schluckt-israelisches-cybersecurity-startup-cyberx-135743/, zuletzt aktualisiert am 22.06.2020, zuletzt geprüft am 03.11.2021.

Jabareen, Hassan; Bishara, Suhad (2019): The Jewish Nation-State Law. In: Journal of Palestine Studies 48 (2), S. 43–57.

Jabareen, Yousef (2018): The nation-state Law and Jewish supremacy. In: Palestine-Israel Journal of Politics, Economics, and Culture 23 (4), S. 16–22.

Jacobs, Ben (2016): Obama says he warned Russia to ›cut it out‹ over election hacking. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/us-news/2016/dec/16/barack-obama-final-press-conference-election-hacking, zuletzt aktualisiert am 16.12.2016, zuletzt geprüft am 11.02.2022.

Jain-Chandra, Sonali; Khor, Niny; Mano, Rui; Schauer, Johanna; Wingender, Philippe; Zhuang, Juzhong (2018): Inequality in China – Trends, Drivers and Policy Remedies. Hg. v. International Monetary Fund (IMF Working Papers, 127). Online verfügbar unter https://books.google.de/books?hl=de&lr=&id=vzBlDwAAQBAJ&oi=fnd&pg=PR4&dq=imf+working+paper+Inequality+in+China+%E2%80%93+Trends,+Drivers+and+Policy+Remedies&ots=2v8qD9s4TN&sig=T9ZARVBWbL7DDWsIe3xK3s1sDCQ, zuletzt geprüft am 25.07.2021.

Jasper, Scott (2021): Assessing Russia's role and responsibility in the Colonial Pipeline attack. Hg. v. Atlantic Council. Online verfügbar unter https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/, zuletzt aktualisiert am 01.06.2021, zuletzt geprüft am 09.06.2021.

Jerusalem Center for Public Affairs (2012): Poll: 77 Percent of Israelis See Iran Nukes as Existential Threat. In: Jerusalem Issue Briefs 12 (4). Online verfügbar unter https://jcpa.org/article/poll-77-percent-of-israelis-see-iran-nukes-as-existential-threat/, zuletzt geprüft am 03.01.2022.

Jervis, Robert (2017): 7. Why Intelligence and Policymakers Clash. In: Robert Jervis (Hg.): How Statesmen Think. The Psychology of International Politics. Princeton: Princeton University Press, S. 148–168.

Jinping, Xi (2018): 习近平在全国组织工作会议上的讲话_共产党员网 [Rede von Xi Jinping auf der National Organization Work Conference]. Hg. v. 12371.CN. Online

verfügbar unter http://www.12371.cn/2018/09/17/ARTI1537150840597467.shtml, zuletzt aktualisiert am 03.07.2018, zuletzt geprüft am 09.07.2021.

Ji-Young, Kong; Jong In, Lim; Kyoung Gon, Kim (2019): The All-Purpose Sword: North Korea's Cyber Operations and Strategies. In: Tomáš Minárik, Siim Alatalu, Stefano Biondi, Massimiliano Signoretti, Ihsan Tolga und Gabor Visky (Hg.): 2019 11th International Conference on Cyber Conflict (CyCon). Tallinn, Estonia: IEEE, S. 1–20.

Johnson, A. L. (2017): BadRabbit: New strain of ransomware hits Russia and Ukraine. Hg. v. Symantec. Online verfügbar unter https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=39104bd6-008d-46a9-bf29-b061c8ecc815&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments, zuletzt aktualisiert am 27.10.2017, zuletzt geprüft am 19.04.2021.

Jones, Jeff (2020): Confronting China's Efforts to Steal Defense Information. Hg. v. Belfer Center for Science and International Affairs. Online verfügbar unter https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information, zuletzt geprüft am 31.07.2021.

Jones, William C. (1985): The Constitution of the People's Republic of China. In: Washington University Law Review 63 (4), S. 707–735.

Joshi, Sahil (2020): Mega Mumbai power outage may be result of cyber attack, final report awaited. Hg. v. India Today. Online verfügbar unter https://www.indiatoday.in/india/story/mumbai-power-outage-malware-attack-1742538-2020-11-20, zuletzt aktualisiert am 20.11.2020, zuletzt geprüft am 23.06.2021.

Kaczmarski, Marcin (2016): The asymmetric partnership? Russia's turn to China. In: International Politics 53 (3), S. 415–434. DOI: 10.1057/ip.2016.7.

Kahl, Colin H. (1998): Constructing a separate peace: Constructivism, collective liberal identity, and democratic peace. In: Security Studies 8 (2–3), S. 94–144. DOI: 10.1080/09636419808429376.

Kahl, Jürgen (2001): Großer Sprung in die Globalisierung: China vor dem Beitritt zur WTO. In: Internationale Politik und Gesellschaft (4), S. 423–434. Online verfügbar unter https://library.fes.de/pdf-files/ipg/ipg-2001-4/artkahl.pdf, zuletzt geprüft am 25.07.2021.

Kailitz, Steffen (2013): Classifying political regimes revisited: legitimation and durability. In: Democratization 20 (1), S. 39–60. DOI: 10.1080/13510347.2013.738861.

Kaminska, Monica (2021): Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks. In: Journal of Cybersecurity 7 (1), Artikel tyab008. DOI: 10.1093/cybsec/tyab008.

Kania, Elsa B.; Costello, John K. (2018): The strategic support force and the future of chinese information operations. In: The Cyber Defense Review 3 (1), S. 105–122.

Kannunikova, Tatiana (2021): Gil Shwed, Co-Founder & CEO of Check Point Software Technologies Ltd | Company & CEO Profile. Hg. v. Gadgets Reviews. Online verfügbar unter https://gadgets-reviews.com/company-ceo-profiles/5706-heck-point-software-technologies.html, zuletzt aktualisiert am 12.05.2021, zuletzt geprüft am 11.10.2021.

Kant, Immanuel (1795): Zum ewigen frieden. In: Ein philosophischer Entwurf.

Kaspersky (2018): A Slice of 2017 Sofacy Activity. Hg. v. Securelist. Kaspersky. Online verfügbar unter https://securelist.com/a-slice-of-2017-sofacy-activity/83930/, zuletzt aktualisiert am 20.02.2018.

Kastein, Julia (2020): Endspurt im US-Wahlkampf – Trumps Versprechen für den Rust Belt. Hg. v. Deutschlandfunk Kultur. Online verfügbar unter https://www.deutschlandfunkkultur.de/endspurt-im-us-wahlkampf-trumps-versprechen-fuer-den-rust.979.de.html?dram:article_id=485779, zuletzt aktualisiert am 15.10.2020, zuletzt geprüft am 27.09.2021.

Katz, Yaakov (2010): ›Stuxnet virus set back Iran's nuclear program by 2 years‹. Hg. v. The Jerusalem Post. Online verfügbar unter https://www.jpost.com/iranian-threat/news/stuxnet-virus-set-back-irans-nuclear-program-by-2-years, zuletzt aktualisiert am 15.12.2010.

Kelle, Udo (2014): Mixed Methods. In: Nina Baur und Jörg Blasius (Hg.): Handbuch Methoden der empirischen Sozialforschung: Springer, S. 153–166.

Kenyon, Miles (2018): The NSO connection to Jamal Khashoggi. Hg. v. The Citizen Lab. Online verfügbar unter https://citizenlab.ca/2018/10/the-nso-connection-to-jamal-khashoggi/, zuletzt aktualisiert am 24.10.2018, zuletzt geprüft am 26.10.2021.

Keohane, Robert O. (1984): After hegemony: Cooperation and discord in the world political economy. Princeton, Oxford: Princeton University Press.

Keohane, Robert O.; Martin, Lisa L. (1995): The promise of institutionalist theory. In: International Security 20 (1), S. 39–51.

Keohane, Robert O.; Nye, Joseph S. (1987): Power and Interdependence revisited. In: International Organization 41 (4), S. 725–753.

Keohane, Robert O.; Nye, Joseph S.; Zakaria, Fareed (2012): Power and interdependence. 4. ed. Boston: Longman (Longman classics in political science).

Keohane, Robert O.; Nye Jr, Joseph S. (1998): Power and interdependence in the information age. In: Foreign Affairs 77, S. 81.

Keohane, Robert Owen (2002): Power and governance in a partially globalized world. London, New York: Routledge. Online verfügbar unter http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=96854.

Khan, Muqtedar (2018): Israel: No More the ›Only Democracy in the Middle East‹. Hg. v. Center for Global Policy. Online verfügbar unter https://www.cgpolicy.org/articles/israel-no-longer-the-only-democracy-in-the-middle-east/.

Kharpal, Arjun (2018): A major factor behind the US-China trade war is winning at a $12 trillion technology – 5G. Hg. v. CNBC. Online verfügbar unter https://www.cnbc.com/2018/07/06/a-major-factor-behind-the-us-china-trade-war-is-winning-in-a-crucial-t.html, zuletzt aktualisiert am 06.07.2018, zuletzt geprüft am 06.10.2021.

King, Gary; Keohane, Robert O.; Verba, Sidney (1994): Designing social inquiry: Scientific inference in qualitative research: Princeton University Press.

King, Gary; Pan, Jennifer; Roberts, Margaret E. (2013): How censorship in China allows government criticism but silences collective expression. In: American Political Science Review 107 (2), S. 326–343.

King & Spalding (2015): U.S. Business Groups Urge Obama Administration To Address Chinese Cybersecurity Rules | JD Supra. Hg. v. JD Supra. Online verfügbar unter

https://www.jdsupra.com/legalnews/u-s-business-groups-urge-obama-11440/, zuletzt aktualisiert am 20.08.2015, zuletzt geprüft am 02.09.2021.

Kingsley, Patrick (2021): Israel Security Chief Warns Against Incitement of Conflict as Tensions Mount Before Key Vote. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2021/06/06/world/israel-security-chief-warning-incitement.html, zuletzt aktualisiert am 06.06.2021, zuletzt geprüft am 05.01.2022.

Kirchgaessner, Stephanie; Lewis, Paul; Pegg, David; Cutler, Sam; Lakhani, Nina; Safi, Michael (2021): Revealed: leak uncovers global abuse of cyber-surveillance weapon. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus, zuletzt aktualisiert am 18.07.2021, zuletzt geprüft am 26.10.2021.

Kirkpatrick, David D.; Mazzetti, Mark (2018): How 2 Gulf Monarchies Sought to Influence the White House. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2018/03/21/us/politics/george-nader-elliott-broidy-uae-saudi-arabia-white-house-influence.html?mtrref=undefined&auth=login-email, zuletzt aktualisiert am 21.03.2018, zuletzt geprüft am 06.10.2021.

Kjøllesdal, Kristian Aamelfot; Welle-Strand, Anne (2010): Foreign Aid Strategies: China Taking Over? In: Asian Social Science 6 (10). DOI: 10.5539/ass.v6n10p3.

Klare, Michael T. (1989): Subterranean alliances: America's global proxy network. In: Journal of International Affairs, S. 97–118.

Kleinsteiber, Meghan (2013): Nationalism and Domestic Politics as Drivers of Maritime Conflict. In: The SAIS Review of International Affairs 33 (2), S. 15–19. Online verfügbar unter https://www.jstor.org/stable/26995397.

Klimburg, Alexander (2011): Mobilising Cyber Power. In: Survival 53 (1), S. 41–60. DOI: 10.1080/00396338.2011.555595.

Knake, Robert K. (2010): Untangling attribution: Moving to accountability in cyberspace. Hg. v. Council on Foreign Relations (Prepared Statement before the Subcommittee on Technology and Innovation, Committee on Science and Technology, Hearing: Planning for the Future of Cyber Attack.).

Knop, Dirk (2022): Cybergang Conti: Interne Daten geleakt – 2,8 Milliarden US-Dollar erbeutet. Hg. v. Heise Online. Online verfügbar unter https://www.heise.de/news/Cybergang-Conti-Interne-Daten-geleakt-2-8-Milliarden-US-Dollar-erbeutet-6529035.html, zuletzt aktualisiert am 03.01.2022, zuletzt geprüft am 15.12.2022.

Knott, Stephen F. (2014): The CIA's Greatest Fear: Being Thrown Under the Bus by Congress…Again. Hg. v. The National Interest. Online verfügbar unter https://nationalinterest.org/feature/the-cia%E2%80%99s-greatest-fear-being-thrown-under-the-bus-by-11034, zuletzt aktualisiert am 08.08.2014, zuletzt geprüft am 11.01.2022.

Koshkin, Roman (2021): Israeli Military Construction: The Financial Aspect. In: New Defence Order Strategy 69 (4). Online verfügbar unter https://dfnc.ru/en/journal/2021-4-69/israeli-military-construction-the-financial-aspect/, zuletzt geprüft am 02.01.2022.

Kostyuk, Nadiya; Zhukov, Yuri M. (2019): Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? In: Journal of Conflict Resolution 63 (2), S. 317–347. DOI: 10.1177/0022002717737138.

Kotkin, Joel (2012): Despite the Great Recession, Obama's New Coalition of Elites Has Thrived. Hg. v. The Daily Beast. Online verfügbar unter https://www.thedailybeast.com/despite-the-great-recession-obamas-new-coalition-of-elites-has-thrived, zuletzt aktualisiert am 14.07.2017, zuletzt geprüft am 02.09.2021.

Kovacs, Eduard (2016): Attack on Swiss Defense Firm Linked to Turla Cyberspies. Hg. v. Securityweek. Online verfügbar unter https://www.securityweek.com/attack-swiss-defense-firm-linked-turla-cyberspies, zuletzt aktualisiert am 23.05.2016, zuletzt geprüft am 14.04.2021.

Krebs, Brian (2014): Hackers Plundered Israeli Defense Firms that Built ›Iron Dome‹ Missile Defense System – Krebs on Security. Hg. v. Krebs on Security. Online verfügbar unter https://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system/, zuletzt aktualisiert am 28.07.2014, zuletzt geprüft am 25.05.2021.

Krebs, Brian (2015): Premera Blue Cross Breach Exposes Financial, Medical Records. Hg. v. Krebs on Security. Online verfügbar unter https://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/, zuletzt aktualisiert am 17.03.2015, zuletzt geprüft am 19.08.2021.

Krebs, Brian (2017): A Shakeup in Russia's Top Cybercrime Unit. Hg. v. Krebs on Security. Online verfügbar unter https://krebsonsecurity.com/2017/01/a-shakeup-in-russias-top-cybercrime-unit/, zuletzt aktualisiert am 28.01.2017, zuletzt geprüft am 06.05.2021.

Krebs, Brian (2022): Russia to Rent Tech-Savvy Prisoners to Corporate IT? Hg. v. Krebs on Security. Online verfügbar unter https://krebsonsecurity.com/2022/05/russia-to-rent-tech-savvy-prisoners-to-corporate-it/, zuletzt aktualisiert am 02.05.2022, zuletzt geprüft am 15.12.2022.

Krekel, Bryan (2009): Capability of the People's Republic of China to conduct cyber warfare and computer network exploitation. Northrop Grumman. Online verfügbar unter https://apps.dtic.mil/dtic/tr/fulltext/u2/a509000.pdf, zuletzt aktualisiert am 2009, zuletzt geprüft am 10.06.2020.

Kremlin.ru (2012): Заседание Совета по межнациональным отношениям [Sitzung des Rates für interethnische Beziehungen]. Hg. v. Kremlin.ru. Online verfügbar unter http://www.kremlin.ru/events/president/news/16292, zuletzt aktualisiert am 24.08.2012, zuletzt geprüft am 05.05.2021.

Kreps, Sarah; Schneider, Jacquelyn (2019): Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics. In: Journal of Cybersecurity 5 (1), Artikel tyz007. DOI: 10.1093/cybsec/tyz007.

Krumm, Reinhard (2010): Der Medwedew-Faktor. Russlands gewünschte Modernisierung. Hg. v. Friedrich-Ebert-Stiftung (Internationale Politikanalyse). Online verfügbar unter http://library.fes.de/pdf-files/id/ipa/07482.pdf, zuletzt aktualisiert am September 2010, zuletzt geprüft am 19.05.2021.

Kryshtanovskaya, Olga; White, Stephen (2003): Putin's militocracy. In: Post-Soviet Affairs 19 (4), S. 289–306.

Kshetri, Nir (2013): Cybercrimes in the Former Soviet Union and Central and Eastern Europe: current status and key drivers. In: Crime Law Soc Change 60 (1), S. 39–65. DOI: 10.1007/s10611-013-9431-4.

Kuhn, Johannes (2010): »Die Büchse der Pandora ist geöffnet«. Hg. v. Süddeutsche Zeitung. Online verfügbar unter https://www.sueddeutsche.de/digital/interview-zum-stuxnet-sabotagevirus-die-buechse-der-pandora-ist-geoeffnet-1.1005985, zuletzt aktualisiert am 03.10.2010, zuletzt geprüft am 26.08.2021.

Kuzio, Taras (2021): Five reasons why Ukraine rejected Vladimir Putin's »Russian World«. Hg. v. Atlantic Council. Online verfügbar unter https://www.atlanticcouncil.org/blogs/ukrainealert/five-reasons-why-ukraine-rejected-vladimir-putins-russian-world/, zuletzt aktualisiert am 26.03.2021, zuletzt geprüft am 06.05.2021.

Lacquement, Richard A. (2004): The casualty-aversion myth. In: Naval War College Review 57 (1), S. 38–58.

Lakshmanan, Ravie (2021): Ukraine Identifies Russian FSB Officers Hacking As Gamaredon Group. Hg. v. The Hacker News. Online verfügbar unter https://thehackernews.com/2021/11/ukraine-identifies-russian-fsb-officers.html, zuletzt aktualisiert am 10.02.2022, zuletzt geprüft am 05.11.2021.

Landler, Mark (2018): Trump Abandons Iran Nuclear Deal He Long Scorned. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2018/05/08/world/middleeast/trump-iran-nuclear-deal.html, zuletzt aktualisiert am 08.05.2018, zuletzt geprüft am 06.10.2021.

Laughlin, Shepherd (2008): Educational exchange between the United States and China. Hg. v. Institute of International Education (An IIE Briefing Paper), zuletzt geprüft am 05.07.2021.

Lebahn, Axel (2010): Modernisierer statt Marionette. Wie Dmitri Medwedew Russlands Politik sanft revolutioniert. In: Internationale Politik (September/Oktober). Online verfügbar unter https://internationalepolitik.de/system/files/article_pdfs/9_10_2010_Lebahn.pdf, zuletzt geprüft am 19.05.2021.

Lee, Heajune (2021): Strategic Publicity?: Understanding US Government Cyber Attribution. Stanford University. Online verfügbar unter https://stacks.stanford.edu/file/druid:py070wt8487/Lee_thesis.pdf, zuletzt geprüft am 08.02.2022.

Lee, John (2018): China's Trojan Ports. Hg. v. Hudson Institute. Online verfügbar unter https://www.hudson.org/research/14717-china-s-trojan-ports, zuletzt aktualisiert am 29.11.2018, zuletzt geprüft am 04.08.2021.

Lee, Robert (2016): The Problems with Seeking and Avoiding True Attribution to Cyber Attacks. Online verfügbar unter https://www.robertmlee.org/the-problems-with-seeking-and-avoiding-true-attribution-to-cyber-attacks/, zuletzt aktualisiert am 04.03.2016.

Lee, Yimou (2020): Taiwan says China behind cyberattacks on government agencies, emails. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-taiwan-cyber-china/taiwan-says-china-behind-cyberattacks-on-government-agencies-emails-idUSKCN25F0JK, zuletzt aktualisiert am 19.08.2020, zuletzt geprüft am 16.06.2021.

Legal Information Institute (2020): Separation of Powers and Checks and Balances. Hg. v. Cornell Law School. Online verfügbar unter https://www.law.cornell.edu/constitution-conan/article-1/section-1/separation-of-powers-and-checks-and-balances, zuletzt aktualisiert am 28.01.2020, zuletzt geprüft am 25.08.2021.

Legro, Jeffrey W. (1996): Culture and preferences in the international cooperation two-step. In: Am Polit Sci Rev 90 (1), S. 118–137.

Leiner, Barry M.; Cerf, Vinton G.; Clark, David D.; Kahn, Robert E.; Kleinrock, Leonard; Lynch, Daniel C. et al. (2009): A brief history of the Internet. In: ACM SIGCOMM Computer Communication Review 39 (5), S. 22–31.

Leipziger Volkszeitung (2018): Festakt im Alten Senatssaal – Konfuzius-Institut Leipzig feiert Zehnjähriges. Hg. v. Leipziger Volkszeitung. Online verfügbar unter https://www.lvz.de/Leipzig/Lokales/Konfuzius-Institut-Leipzig-feiert-Zehnjaehriges, zuletzt aktualisiert am 11.04.2018, zuletzt geprüft am 27.07.2021.

Levada (2021): Indicators. Putin's Approval Rating. Hg. v. Levada. Online verfügbar unter https://www.levada.ru/en/ratings/, zuletzt aktualisiert am 2021, zuletzt geprüft am 06.05.2021.

Levin, Dov H. (2020): Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions: Oxford University Press.

Levitsky, Steven; Ziblatt, Daniel (2018): Wie Demokratien sterben. Und was wir dagegen tun können. München: Deutsche Verlags-Anstalt.

Levy, Ari (2021): Cybereason CEO told the world about DarkSide's hacking techniques from a bomb shelter in Israel. Hg. v. CNBC. Online verfügbar unter https://www.cnbc.com/2021/05/27/cybereason-ceo-was-in-israel-bomb-shelter-telling-world-about-darkside.html, zuletzt aktualisiert am 27.05.2021, zuletzt geprüft am 11.10.2021.

Levy, Jack S. (2008): Case studies: Types, designs, and logics of inference. In: Conflict Management and Peace Science 25 (1), S. 1–18.

Lewis, James (2011): Cyberwar Thresholds and Effects. In: IEEE Secur. Privacy Mag. 9 (5), S. 23–29. DOI: 10.1109/MSP.2011.25.

Lewis, James A. (2014): National perceptions of cyber threats. In: Strategic Analysis 38 (4), S. 566–576.

Lewis, Jason (2015): Cyber Espionage as a Component of Russian Modern Warfare. Hg. v. LookingGlass. Online verfügbar unter https://lookingglasscyber.com/blog/threat-intelligence-insights/operation-armageddon-cyber-espionage-as-a-strategic-component-of-russian-modern-warfare/, zuletzt aktualisiert am 28.04.2015, zuletzt geprüft am 01.01.2022.

Leyden, John (2013): APT1, that scary cyber-Cold War gang: Not even China's best. Hg. v. The Register. Online verfügbar unter https://www.theregister.com/2013/02/27/apt1_china_dark_visitor_b_team/, zuletzt aktualisiert am 27.02.2013, zuletzt geprüft am 14.11.2021.

Libicki, Martin C. (2018): Drawing Inferences from Cyber Espionage. In: T. Minárik, R. Jakschis und L. Lindström (Hg.): CyCon X: Maximising Effects. Tallinn: NATO CCD COE Publications (International Conference on Cyber Conflict, 10), S. 109–122.

Lijphart, Arend (2012): Patterns of democracy: Government forms and performance in thirty-six countries: Yale University Press.

Lim, Kheng Swe (2016): China's nationalist narrative of the South China Sea: A preliminary analysis. In: Enrico Fels und Truong-Minh Vu (Hg.): Power Politics in Asia's Contested Waters. Territorial Disputes in the South China Sea: Springer, S. 159–172.

Lin, Herbert (2016): From Soup to Nuts. Attribution of Malicious Cyber Incidents. In: Journal of International Affairs 70 (1), S. 75–137. Online verfügbar unter http://www.jstor.org/stable/90012598.

Lin, Herbert S. (2010): Offensive cyber operations and the use of force. In: Journal of National Security Law and Policy 4, S. 63–86.

Lindsay, Jon R. (2015): Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. In: Journal of Cybersecurity 1 (1), 53–67. DOI: 10.1093/cybsec/tyv003.

Lipman, Maria (2006): Putin's »Sovereign Democracy«. Hg. v. Carnegie Moscow Center – Carnegie Endowment for International Peace. Carnegie Moscow Center – Carnegie Endowment for International Peace. Online verfügbar unter https://carnegie.ru/2006/07/15/putin-s-sovereign-democracy-pub-18540, zuletzt aktualisiert am 15.07.2006, zuletzt geprüft am 05.05.2021.

Lipton, Eric; Sanger, David E.; Shane, Scott (2016): The Perfect Weapon: How Russian Cyberpower Invaded the U.S. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0, zuletzt aktualisiert am 13.12.2016, zuletzt geprüft am 20.08.2021.

Lloyd's Market Association (2021): Cyber War and Cyber Operation Exclusion Clauses. Hg. v. Lloyd's Market Association Bulletin. Online verfügbar unter https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx, zuletzt aktualisiert am 25.11.2021, zuletzt geprüft am 12.02.2022.

Lockheed Martin (2020): The Cyber Kill Chain. Hg. v. Lockheed Martin. Online verfügbar unter https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Locks, Benjamin (2015): Asymmetric Warfare and the Third Offset – War on the Rocks. Hg. v. War on the Rocks. Online verfügbar unter https://warontherocks.com/2015/06/bad-guys-know-what-works-asymmetric-warfare-and-the-third-offset/, zuletzt aktualisiert am 23.06.2015, zuletzt geprüft am 01.09.2021.

Lohmann, Sarah (2018): Second Roundtable Looks at Role of Private Sector and Civil Society in Attribution – AICGS. Hg. v. American Institute for Contemporary German Studies. John Hopkins University. Online verfügbar unter https://www.aicgs.org/2018/06/second-roundtable-looks-at-role-of-private-sector-and-civil-society-in-attribution/, zuletzt aktualisiert am 28.06.2018, zuletzt geprüft am 18.Ma 2020.

Lohmann, Susanne (1997): Linkage Politics. In: Journal of Conflict Resolution 41 (1), S. 38–67. Online verfügbar unter http://www.jstor.org/stable/174486.

Lonergan, Erica D.; Lonergan, Shawn W. (2022): What do Russia's cyber moves mean for the Ukraine crisis? Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/politics/2022/01/12/what-do-russias-cyber-moves-mean-ukraine-crisis/, zuletzt aktualisiert am 12.01.2022, zuletzt geprüft am 13.01.2022.

Lonsdale, David J. (2019): We aren't in a cyber war – despite what Britain's top general thinks. Hg. v. The Conversation. Online verfügbar unter http://theconversation.com/we-arent-in-a-cyber-war-despite-what-britains-top-general-thinks-125578, zuletzt aktualisiert am 25.10.2019.

Lookout (2019): Monokle. The Mobile Surveillance Tooling of the Special Technology Center. Hg. v. Lookout (Security Research Report). Online verfügbar unter https://www.lookout.com/documents/threat-reports/lookout-discovers-monokle-threat-report.pdf?utm_source=BL&utm_medium=BL&utm_campaign=WW-MU-MU-MU-MU-P_NON-&utm_content=WP_Monokole%20.xml, zuletzt aktualisiert am Juli 2019.

Lösche, Peter (2008): Dossier USA. Hg. v. Bundeszentrale für Politische Bildung. Online verfügbar unter https://www.bpb.de/internationales/amerika/usa/10640/praesidialdemokratie?p=all, zuletzt aktualisiert am 02.10.2008, zuletzt geprüft am 25.08.2021.

Lotrionte, Catherine (2014): Countering state-sponsored cyber economic espionage under international law. In: NCJ Int'l L. & Com. Reg. 40, S. 443.

Lupovici, Amir (2016): The »Attribution Problem« and the Social Construction of »Violence«: Taking Cyber Deterrence Literature a Step Forward. In: International Studies Perspectives 17, 322–342. DOI: 10.1111/insp.12082.

Lyngaas, Sean (2018): DOJ indictment spotlights China's civilian intel agency – and its hacker recruits. Hg. v. Cyberscoop. Online verfügbar unter https://www.cyberscoop.com/ministry-of-state-security-china-hacking-department-of-justice-indictment/, zuletzt aktualisiert am 01.11.2018, zuletzt geprüft am 30.06.2021.

MacAskill, Ewen (2005): George Bush: ›God told me to end the tyranny in Iraq‹. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2005/oct/07/iraq.usa, zuletzt aktualisiert am 07.10.2005, zuletzt geprüft am 01.09.2021.

Machtiger, Peter (2020): The Latest GRU Indictment: A Failed Exercise in Deterrence. Hg. v. Just Security. Online verfügbar unter https://www.justsecurity.org/73071/the-latest-gru-indictment-a-failed-exercise-in-deterrence/, zuletzt aktualisiert am 29.10.2020, zuletzt geprüft am 20.08.2021.

Macias, Amanda (2020): Former cybersecurity chief says Russia, China, Iran and North Korea are trying to steal coronavirus vaccine IP. Hg. v. CNBC. Online verfügbar unter https://www.cnbc.com/2020/12/06/former-top-cybersecurity-chief-says-russia-china-iran-and-north-korea-are-trying-to-steal-coronoavir.html, zuletzt aktualisiert am 06.12.2020, zuletzt geprüft am 25.05.2021.

Magistretti, Bérénice (2017): Cybersecurity startup SentinelOne raises $70 million. Hg. v. Venture Beat. Online verfügbar unter https://venturebeat.com/2017/01/25/cybersecurity-startup-sentinelone-raises-70-million/, zuletzt aktualisiert am 25.01.2017, zuletzt geprüft am 03.11.2021.

Mahoney, James (2010): After KKV: The new methodology of qualitative research. In: World Pol 62, S. 120.

Makarin, Alexey (2019): Политический патриарх. Чего достиг и не достиг Кирилл за десять лет [Politischer Patriarch. Was Kyrill in zehn Jahren erreicht hat und was nicht]. Hg. v. Republic.ru. Online verfügbar unter https://republic.ru/posts/92948, zuletzt aktualisiert am 31.01.2019, zuletzt geprüft am 06.05.2021.

MANDIANT (2010): M-Trends. The Advanced Persistent Threat. Hg. v. Ryan Maness. Online verfügbar unter https://www2.fireeye.com/rs/fireye/images/PDF_MTrends_2010.pdf?mkt_tok=ODQ4LURJRC0yNDIAAAF-BTQAsGyLhrJemwrWOWxn9WjCCSlCipH5bPyPIGKwcu6YCacpq7YK5wqhilsvpj_tnTRGXXrbroP7mc1BAs3MIlRj7PUNiei8F1cnYVcaJ0ETOdY, zuletzt geprüft am 02.07.2021.

MANDIANT (2013): APT1: Exposing one of China's cyber espionage units. Hg. v. MANDIANT. Online verfügbar unter https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf, zuletzt aktualisiert am 19.02.2013, zuletzt geprüft am 25.05.2021.

Maness, Ryan; Valeriano, Brandon (2016a): Cyber spillover conflicts: transitions from cyber conflict to conventional foreign policy disputes? In: Karsten Friis und Jens Ringsmose (Hg.): Conflict in Cyber Space. Theoretical, Strategic and Legal Perspectives. London: Routledge, S. 45–64.

Maness, Ryan C.; Valeriano, Brandon (2016b): The Impact of Cyber Conflict on International Interactions. In: Armed Forces & Society 42 (2), S. 301–323. DOI: 10.1177/0095327X15572997.

Maness, Ryan C.; Valeriano, Brandon; Jensen, Benjamin (2019): Codebook for the Dyadic Cyber Incident and Campaign Dataset (DCID) Version 1.5. Online verfügbar unter http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/dcid_1.5_codebook.pdf, zuletzt aktualisiert am 01.06.2019.

Mangott, Gerhard (2012): Kommentar: Kampfrhetorik und »saubere Siege« Die ausgestreckte Hand Putins ist unabdingbar. Hg. v. Bundeszentrale für Politische Bildung. Online verfügbar unter https://www.bpb.de/internationales/europa/russland/analysen/135752/kommentar-kampfrhetorik, zuletzt aktualisiert am 11.05.2012, zuletzt geprüft am 29.04.2021.

Mankoff, Jeffrey (2014): Russia's latest land grab: How Putin won Crimea and lost Ukraine. In: Foreign Affairs (May/June), S. 60–68. Online verfügbar unter https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/fora93§ion=65.

Manutscharjan, Aschot L. (2017): Russlands Weg in die »postwestliche Welt«. In: Aus Politik und Zeitgeschichte 67 (21–22), S. 11–15.

Mao, Yexin (2021): Political institutions, state capacity, and crisis management: A comparison of China and South Korea. In: International Political Science Review (42), Artikel 3, 316–332.

Marczak, Bill; Anstis, Siena; Crete-Nishihata, Masashi; Scott-Railton, John; Deibert, Ron (2020): Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator – The Citizen Lab. Hg. v. The Citizen Lab. Online verfügbar unter https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/, zuletzt aktualisiert am 29.10.2020, zuletzt geprüft am 26.10.2021.

Marczak, Bill; Scott-Railton, John (2016): The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender – The Citizen Lab. Hg. v. The Citizen Lab. Online verfügbar unter https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/, zuletzt aktualisiert am 24.08.2016, zuletzt geprüft am 26.10.2021.

Maréchal, Nathalie (2017): Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. In: MaC 5 (1), S. 29–41. DOI: 10.17645/mac.v5i1.808.

Maresca, Thomas (2014): Obama: Goal is not to ›contain‹ China. Hg. v. USA Today. Online verfügbar unter https://eu.usatoday.com/story/news/world/2014/04/28/obama

-philippines-china/8403801/, zuletzt aktualisiert am 28.04.2014, zuletzt geprüft am 02.08.2021.

Marks, Joseph (2019): The Cybersecurity 202: Russia's false flags in Winter Olympics cyberattack herald a more complicated future. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/10/21/the-cybersecurity-202-russia-s-false-flags-in-winter-olympics-cyberattack-herald-a-more-complicated-future/5dac9e2888e0fa3155a71266/, zuletzt aktualisiert am 17.07.2020, zuletzt geprüft am 18.04.2021.

Marks, Joseph (2020): The Cybersecurity 202: Chinese hackers could work for the government – or themselves. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/politics/2020/07/22/cybersecurity-202-chinese-hackers-could-work-government-or-themselves/, zuletzt aktualisiert am 22.07.2020, zuletzt geprüft am 01.07.2021.

Marks, Joseph (2022): The U.S.-Russia cyber relationship just got even more complicated. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/politics/2022/01/18/us-russia-cyber-relationship-just-got-even-more-complicated/, zuletzt aktualisiert am 18.01.2022, zuletzt geprüft am 24.01.2022.

Markus, Stanislav (2017): The Atlas That has Not Shrugged: Why Russia's Oligarchs are an Unlikely Force for Change. In: Daedalus 146 (2), S. 101–112.

Marquardt, Alex; Perez, Evan; Cohen, Zachary; Stracqualursi, Veronica (2020): Intel community's top election official: China and Iran don't want Trump to win reelection, Russia working to ›denigrate‹ Biden. Hg. v. CNN. Online verfügbar unter https://edition.cnn.com/2020/08/07/politics/2020-election-russia-china-iran/index.html, zuletzt aktualisiert am 08.08.2020, zuletzt geprüft am 07.01.2022.

Marshall, Alex (2016): From civil war to proxy war: past history and current dilemmas. In: Small wars & insurgencies 27 (2), S. 183–195. DOI: 10.1080/09592318.2015.1129172.

Marten, Kimberly (2017): The ›KGB State‹ and Russian Political and Foreign Policy Culture. In: The Journal of Slavic Military Studies 30 (2), S. 131–151. DOI: 10.1080/13518046.2017.1270053.

Marten, Kimberly (2019): Russia's use of semi-state security forces: the case of the Wagner Group. In: Post-Soviet Affairs 35 (3), S. 181–204. DOI: 10.1080/1060586X.2019.1591142.

Maschmeyer, Lennart; Deibert, Ronald J.; Lindsay, Jon R. (2020): A tale of two cybers – how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. In: Journal of Information Technology & Politics, S. 1–20. DOI: 10.1080/19331681.2020.1776658.

Maschmeyer, Lennart; Kostyuk, Nadiya (2022): There Is No Cyber ›Shock and Awe‹: Plausible Threats in the Ukrainian Conflict. Hg. v. War on the Rocks. Online verfügbar unter https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/, zuletzt aktualisiert am 08.02.2022, zuletzt geprüft am 10.02.2022.

Mattes, Michaela; Rodríguez, Mariana (2014): Autocracies and International Cooperation. In: International Studies Quarterly 58 (3), S. 527–538. DOI: 10.1111/isqu.12107.

Mattingly, Daniel C. (2021): How the Party Commands the Gun: The Foreign-Domestic Threat Dilemma in China. Online verfügbar unter https://static1.squarespace.com/static/51cdc7e5e4b0d7474642bcb0/t/60f8809a47dddc167f011a3e/1626898586392/

Mattingly_PLA_Paper.pdf, zuletzt aktualisiert am 21.07.2021, zuletzt geprüft am 25.07.2021.

Mattis, Peter (2015a): A Guide to Chinese Intelligence Operations – War on the Rocks. Hg. v. War on the Rocks. Online verfügbar unter https://warontherocks.com/2015/08/a-guide-to-chinese-intelligence-operations/, zuletzt aktualisiert am 18.08.2015, zuletzt geprüft am 30.06.2021.

Mattis, Peter (2015b): Chen Wenqing: China's New Man for State Security. Hg. v. The National Interest. Online verfügbar unter https://nationalinterest.org/feature/chen-wenqing-china%E2%80%99s-new-man-state-security-14153, zuletzt aktualisiert am 23.10.2015, zuletzt geprüft am 25.07.2021.

Maull, Hanns W. (2022): Ukraine and Taiwan: two conflict zones with destabilizing potential. Hg. v. Merics. Online verfügbar unter https://merics.org/en/opinion/ukraine-and-taiwan-two-conflict-zones-destabilizing-potential, zuletzt aktualisiert am 04.02.2022, zuletzt geprüft am 10.02.2022.

Maurer, Tim (2011): Cyber norm emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security? Cambridge, Mass. (Discussion Paper, 2011–11).

Maurer, Tim (2016): ›Proxies‹ and Cyberspace. In: Journal of Conflict and Security Law 21 (3), S. 383–403. DOI: 10.1093/jcsl/krw015.

Maurer, Tim (2018a): Cyber Mercenaries. Cambridge: Cambridge University Press.

Maurer, Tim (2018b): Cyber Proxies and Their Implications for Liberal Democracies. In: The Washington Quarterly 41 (2), S. 171–188. DOI: 10.1080/0163660X.2018.1485332.

Mccrimmon, Ryan; Matishak, Martin (2021): Cyberattack on food supply followed years of warnings. Hg. v. Politico. Online verfügbar unter https://www.politico.com/news/2021/06/05/how-ransomware-hackers-came-for-americans-beef-491936, zuletzt aktualisiert am 05.06.2021, zuletzt geprüft am 02.09.2021.

McGuire, Michael (2021): Nation States, Cyberconflict and the Web of Profit. Hg. v. HP Threat Research. Online verfügbar unter https://threatresearch.ext.hp.com/web-of-profit-nation-state-report/.

McNamara, Luke (2021): The »Big Four«: Spotlight on Russia. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/blog/executive-perspective/2021/04/the-big-four-spotlight-on-russia.html, zuletzt aktualisiert am 12.04.2021, zuletzt geprüft am 19.08.2021.

Mehrotra, Kartikay (2021): Microsoft Weighs Fixes to Code-Sharing Plan After Suspected Leak. Hg. v. Bloomberg. Online verfügbar unter https://www.bloomberg.com/news/articles/2021-04-27/microsoft-weighs-revamping-flaw-disclosures-after-suspected-leak, zuletzt aktualisiert am 27.04.2021, zuletzt geprüft am 02.07.2021.

Mell, Peter; Scarfone, Karen; Romanosky, Sasha (2007): A Complete Guide to the Common Vulnerability Scoring System. Version 2.0. FIRST.ORG, Inc. Online verfügbar unter https://www.first.org/cvss/v2/guide, zuletzt aktualisiert am 15.06.2019, zuletzt geprüft am 31.03.2020.

Melzer, Nils (2008): Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law. Hg. v. International Committee of the Red Cross. International Committee of the Red Cross. Genf. Online

verfügbar unter https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf, zuletzt geprüft am 18.05.2020.

Meng, Anne (2021): Winning the Game of Thrones: Leadership Succession in Modern Autocracies. In: Journal of Conflict Resolution 65 (5), S. 950–981.

Mercer, Andrew; Deane, Claudia; Mcgeeney, Kyley (2016): Why 2016 election polls missed their mark. Hg. v. Pew Research Center. Online verfügbar unter https://www.pewresearch.org/fact-tank/2016/11/09/why-2016-election-polls-missed-their-mark/, zuletzt aktualisiert am 09.11.2016, zuletzt geprüft am 08.09.2021.

Merkel, Wolfgang (1999): Die drei Demokratisierungswellen des 20. Jahrhunderts. In: Wolfgang Merkel (Hg.): Systemtransformation. Eine Einführung in die Theorie und Empirie der Transformationsforschung. Wiesbaden, s.l.: VS Verlag für Sozialwissenschaften (Beiträge zur Kenntnis des Rechtslebens, 2076), S. 173–184.

Merkel, Wolfgang (2004): Embedded and defective democracies. In: Democratization 11 (5), S. 33–58.

Merkley, Jeff; McGovern, James P. (2006): Ministry of Public Security Urges Use of »Strike Hard« to Counter Social Unrest. Hg. v. Congressional-Executive Commission on China. Online verfügbar unter https://www.cecc.gov/publications/commission-analysis/ministry-of-public-security-urges-use-of-strike-hard-to-counter, zuletzt aktualisiert am 22.05.2006, zuletzt geprüft am 27.07.2021.

Mesquita, Bruce Bueno de; Lalman, David (1990): Domestic Opposition and Foreign War. In: American Political Science Review 84 (3), S. 747–765. DOI: 10.2307/1962765.

Mesquita, Bruce Bueno de; Smith, Alastair; Siverson, Randolph M.; Morrow, James D. (2005): The logic of political survival: MIT press.

Meyer, Thomas (2009): Was ist Demokratie? Eine diskursive Einführung. Wiesbaden: VS Verlag für Sozialwissenschaften.

Meyers, Adam (2016): Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units. Hg. v. CrowdStrike. Online verfügbar unter https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/, zuletzt aktualisiert am 22.12.2016.

Michaels, Jon D. (2017): Trump and the »Deep State« The Government Strikes Back. In: Foreign Affairs 96 (5), S. 52–56. Online verfügbar unter http://www.jstor.org/stable/44821868.

Microsoft (2019): Government Security Program. Programmübersicht. Hg. v. Microsoft. Online verfügbar unter https://docs.microsoft.com/de-de/security/gsp/programoverview, zuletzt aktualisiert am 19.02.2019, zuletzt geprüft am 02.07.2021.

Microsoft Security (2021): HAFNIUM targeting Exchange Servers with 0-day exploits – Microsoft Security. Hg. v. Microsoft Security. Online verfügbar unter https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/, zuletzt aktualisiert am 26.03.2021, zuletzt geprüft am 25.05.2021.

Microsoft Threat Intelligence Center (2021): HAFNIUM targeting Exchange Servers with 0-day exploits. Hg. v. Microsoft Security. Online verfügbar unter https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/, zuletzt aktualisiert am 02.03.2021, zuletzt geprüft am 14.11.2021.

Militarist Monitor (2019): Projekt for the New American Century. Hg. v. Militarist Monitor. Online verfügbar unter https://militarist-monitor.org/profile/project_for_th

e_new_american_century/, zuletzt aktualisiert am 16.10.2019, zuletzt geprüft am 25.08.2021.

Miller, Maggie (2021): US concerns grow over potential Russian cyber targeting of Ukraine amid troop buildup. Hg. v. The Hill. Online verfügbar unter https://thehill.com/policy/cybersecurity/586033-us-concerns-grow-over-potential-russian-cyber-targeting-of-ukraine-amid/, zuletzt aktualisiert am 16.12.2021, zuletzt geprüft am 09.12.2022.

Ministry of Defense Israel (2020): Defense Establishment thwarts cyber-attack targeting defense industries 12 August 2020. Hg. v. Israel Ministry of Foreign Affairs. Online verfügbar unter https://mfa.gov.il/MFA/ForeignPolicy/Pages/Defense-Establishment-thwarts-cyber-attack-targeting-defense-industries-12-August-2020.aspx, zuletzt aktualisiert am 12.08.2020, zuletzt geprüft am 12.02.2022.

Mirski, Sean (2015): The South China Sea Dispute: A Brief History. Hg. v. Lawfare. Online verfügbar unter https://www.lawfareblog.com/south-china-sea-dispute-brief-history, zuletzt aktualisiert am 31.10.2019, zuletzt geprüft am 02.08.2021.

Mischke, Judith (2017): Russian hackers behind leak of UN diplomat's email: report. Hg. v. Politico. Online verfügbar unter https://www.politico.eu/article/russian-hackers-fancy-bear-behind-leak-of-un-diplomats-email-report/, zuletzt aktualisiert am 20.11.2017, zuletzt geprüft am 19.04.2021.

Mitchell, Sierra (2021): Profile of Group-IB CEO Ilya Sachkov, who is charged with treason in Russia, sources say for allegedly giving the US info about Fancy Bear's 2016 operation (Bloomberg). Hg. v. News AKMI. Online verfügbar unter https://newsakmi.com/news/tech-news/profile-of-group-ib-ceo-ilya-sachkov-who-is-charged-with-treason-in-russia-sources-say-for-allegedly-giving-the-us-info-about-fancy-bears-2016-operation-bloomberg/, zuletzt aktualisiert am 05.12.2021, zuletzt geprüft am 30.12.2021.

MOD (2011): Kontseptual'nye vzglyady na deyatel'nost‹ Vooruzhennykh Sil Rossiyskoy Federatsii v informatsionnom prostranstve [Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space]. Hg. v. Ministry of Defense of the Russian Federation. Online verfügbar unter http://www.pircenter.org/en/articles/532-conceptual-views-on-the-activity-of-the-armed-forces-of-the-russian-federation-in-information-space, zuletzt geprüft am 27.04.2021.

Moersen, Alex (2018): How Israel Became a Cybersecurity Powerhouse. Hg. v. Innovation & Tech Today. Online verfügbar unter https://innotechtoday.com/israel-cybersecurity-powerhouse/, zuletzt aktualisiert am 23.05.2018, zuletzt geprüft am 25.10.2021.

MOFA (2000): NATIONAL SECURITY CONCEPT OF THE RUSSIAN FEDERATION. Hg. v. The Ministry of Foreign Affairs of the Russian Federation. Online verfügbar unter https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=en_GB, zuletzt aktualisiert am 10.01.2000, zuletzt geprüft am 27.04.2021.

MOFA (2010): Военная доктрина Российской Федерации [Militärdoktrin der Russischen Föderation]. Hg. v. The Ministry of Foreign Affairs of the Russian Federation. Online verfügbar unter http://kremlin.ru/supplement/461, zuletzt aktualisiert am 05.02.2010, zuletzt geprüft am 27.04.2021.

MOFA (2013): Concept of the Foreign Policy of the Russian Federation. Hg. v. The Ministry of Foreign Affairs of the Russian Federation. Online verfügbar unter https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/122186, zuletzt aktualisiert am 18.02.2013, zuletzt geprüft am 27.04.2021.

MOFA (2016): Doctrine of Information Security of the Russian Federation. Hg. v. The Ministry of Forein Affairs of the Russian Federation. Online verfügbar unter https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163, zuletzt aktualisiert am 05.12.2016, zuletzt geprüft am 27.04.2021.

Moghadam, Assaf; Wyss, Michel (2020): The Political Power of Proxies: Why Nonstate Actors Use Local Surrogates. In: International Security 44 (4), S. 119–157. DOI: 10.1162/ISEC_a_00377.

Mommsen, Margareta (2018): Verfassungsordnung versus politische Realität | Dossier Russland. Hg. v. Bundeszentrale für Politische Bildung. Online verfügbar unter https://www.bpb.de/internationales/europa/russland/47940/verfassungsordnung-versus-politische-realitaet, zuletzt aktualisiert am 26.03.2018, zuletzt geprüft am 28.04.2021.

Mommsen, Margareta; Nußberger, Angelika (2007): Das System Putin. Gelenkte Demokratie und politische Justiz in Russland. Originalausgabe ; 2. aktualisierte und erweiterte Auflage. München: Verlag C.H. Beck (Beck'sche Reihe, 1763).

Moran, Ned; Villeneuve, Nart (2013): Operation DeputyDog: Zero-Day (CVE-2013-3893) Attack Against Japanese Targets. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/blog/threat-research/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html, zuletzt aktualisiert am 21.09.2013, zuletzt geprüft am 25.06.2021.

Moravcsik, Andrew (1993): Preferences and power in the European Community: a liberal intergovernmentalist approach. In: JCMS: Journal of Common Market Studies 31 (4), S. 473–524.

Moravcsik, Andrew (1997): Taking preferences seriously: A liberal theory of international politics. In: International Organization 51 (4), S. 513–553.

Moravcsik, Andrew (1998): The choice for Europe: Social purpose and state power from Messina to Maastricht: Routledge.

Moravcsik, Andrew (2000): The origins of human rights regimes: Democratic delegation in postwar Europe. In: International Organization, S. 217–252.

Moravcsik, Andrew (2003): Liberal international relations theory: a scientific assessment. In: Progress in international relations theory: appraising the field, S. 159–204.

Moravcsik, Andrew (2013): The New Liberalism. In: Robert E. Goodin (Hg.): The Oxford Handbook of Political Science. Oxford: Oxford University Press (Oxford Handbooks Online).

Morgan, Steve (2019): Hot 150 Cybersecurity Companies To Watch In 2021. Hg. v. Cybercrime Magazine. Online verfügbar unter https://cybersecurityventures.com/cybersecurity-companies-list-hot-150/#hot-150/?view_15_per_page=150&view_15_page=1, zuletzt aktualisiert am 06.01.2021, zuletzt geprüft am 25.08.2021.

Morgan, Steve (2020): China Cybersecurity Companies. Hg. v. Cybercrime Magazine. Online verfügbar unter https://cybersecurityventures.com/china-cybersecurity-companies/, zuletzt aktualisiert am 15.10.2020, zuletzt geprüft am 07.07.2021.

Moriuchi, Priscilla; Ladd, Bill (2017): China's Ministry of State Security Likely Influences National Network Vulnerability Publications. Hg. v. Recorded Future. Online verfügbar unter https://www.recordedfuture.com/chinese-mss-vulnerability-influence/, zuletzt aktualisiert am 16.11.2017, zuletzt geprüft am 25.06.2021.

Morozov, Evgeny (2011): The dark side of internet freedom: The net delusion. In: New York: Public Affairs.

Mshvidobadze, Khatuna (2011): The Battlefield On Your Laptop. Hg. v. Radio Free Europe. Online verfügbar unter https://www.rferl.org/a/commentary_battlefield_on_your_desktop/2345202.html, zuletzt aktualisiert am 21.03.2011, zuletzt geprüft am 27.04.2021.

Mudde, Cas (2004): The populist zeitgeist. In: Government and opposition 39 (4), S. 541–563.

Mueller, Milton (2017): Will the internet fragment? Sovereignty, globalization and cyberspace. Cambridge, Malden, MA: Polity. Online verfügbar unter https://ebookcentral.proquest.com/lib/gbv/detail.action?docID=4875231.

Mueller, Milton; Grindal, Karl; Kuerbis, Brenden; Badiei, Farzaneh (2019): Cyber Attribution. Can a New Institution Achieve Transnational Credibility? In: The Cyber Defense Review 4 (1), S. 107–122.

Mueller, Milton L. (2020): Against Sovereignty in cyberspace. In: International Studies Review 22 (4), S. 779–801.

Mueller, Robert S. (2019a): Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volume II of II. Hg. v. Special Counsel's Office. Online verfügbar unter https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html, zuletzt geprüft am 20.08.2021.

Mueller, Robert S. (2019b): Report on the Investigation into Russian Interference in the 2016 Presidential Election. Volume I of II. Hg. v. Special Counsel's Office. Online verfügbar unter https://www.justice.gov/archives/sco/file/1373816/download, zuletzt geprüft am 20.08.2021.

Mulvad, Andreas Møller (2019): Xiism as a hegemonic project in the making: Sino-communist ideology and the political economy of China's rise. In: Review of International Studies 45 (3), S. 449–470. DOI: 10.1017/S0260210518000530.

Mumford, Andrew (2013): Proxy Warfare. Hoboken: Wiley.

Muncaster, Phil (2018): Five Eyes Nations United in Blaming Russia for NotPetya. Hg. v. Infosecurity Magazine. Online verfügbar unter https://www.infosecurity-magazine.com/news/five-eyes-united-blaming-russia/, zuletzt aktualisiert am 19.02.2018, zuletzt geprüft am 06.10.2021.

Muncaster, Phil (2019): Dutch Insider Deployed Stuxnet: Report. Hg. v. Infosecurity Magazine. Online verfügbar unter https://www.infosecurity-magazine.com/news/dutch-insider-deployed-stuxnet/, zuletzt aktualisiert am 04.09.2019, zuletzt geprüft am 02.07.2021.

Muth, Max (2019): Die Software, die Whatsapp hacken sollte. Hg. v. Süddeutsche Zeitung. Online verfügbar unter https://www.sueddeutsche.de/digital/spyware-pegasus-nso-group-whatsapp-hack-1.4447562.

Myre, Greg (2020): A ›Perception Hack‹: When Public Reaction Exceeds The Actual Hack. Hg. v. NPR. Online verfügbar unter https://www.npr.org/2020/11/01/929101685/a-perception-hack-when-public-reaction-exceeds-the-actual-hack, zuletzt aktualisiert am 01.11.2020, zuletzt geprüft am 20.05.2021.

Nakashima, Ellen (2013a): Chinese hackers who breached Google gained access to sensitive data, U.S. officials say. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html, zuletzt aktualisiert am 20.05.2013, zuletzt geprüft am 21.06.2021.

Nakashima, Ellen (2013b): Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html, zuletzt aktualisiert am 28.05.2013, zuletzt geprüft am 08.09.2021.

Nakashima, Ellen (2014): Iranian hackers target U.S. officials on Twitter, Facebook and other social networks. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/world/national-security/iranian-hackers-are-targeting-us-officials-through-social-networks-report-says/2014/05/28/7cb86672-e6ad-11e3-8f90-73e071f3d637_story.html?utm_term=.95e99b2d36f7, zuletzt aktualisiert am 29.05.2014, zuletzt geprüft am 12.08.2021.

Nakashima, Ellen (2016): Russian government hackers penetrated DNC, stole opposition research on Trump. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html, zuletzt aktualisiert am 14.06.2016, zuletzt geprüft am 20.08.2021.

Nakashima, Ellen (2017): New details emerge about 2014 Russian hack of the State Department: It was ›hand to hand combat‹. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/world/national-security/new-details-emerge-about-2014-russian-hack-of-the-state-department-it-was-hand-to-hand-combat/2017/04/03/d89168e0-124c-11e7-833c-503e1f6394c9_story.html, zuletzt aktualisiert am 03.04.2017.

Nakashima, Ellen (2020): U.S. undertook cyber operation against Iran as part of effort to secure the 2020 election. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/national-security/cybercom-targets-iran-election-interference/2020/11/03/aa0c9790-1e11-11eb-ba21-f2f001f0554b_story.html, zuletzt aktualisiert am 03.11.2020, zuletzt geprüft am 06.10.2021.

Naraine, Ryan (2010): Microsoft knew of IE zero-day flaw since last September. Hg. v. ZDnet. Online verfügbar unter https://www.zdnet.com/article/microsoft-knew-of-

ie-zero-day-flaw-since-last-september/, zuletzt aktualisiert am 21.01.2010, zuletzt geprüft am 21.06.2021.

NCSC (2018a): Joint US – UK statement on malicious cyber activity carried out by Russian government. Hg. v. National Cyber Security Centre. Online verfügbar unter https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government, zuletzt aktualisiert am 15.11.2018, zuletzt geprüft am 06.10.2021.

NCSC (2018b): Reckless campaign of cyber attacks by Russian military intelligence service exposed. Hg. v. National Cyber Security Centre UK. Online verfügbar unter https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed, zuletzt aktualisiert am 18.03.2020, zuletzt geprüft am 19.04.2021.

Neuberger, Benyamin (2008): Staatsaufbau und politisches System. Hg. v. Bundeszentrale für Politische Bildung. Online verfügbar unter https://www.bpb.de/internationales/asien/israel/45024/das-politische-system, zuletzt aktualisiert am 10.06.2008, zuletzt geprüft am 02.01.2022.

Nevers, Renée de (2016): Private Security's Role in Shaping US Foreign Policy. In: Anna Leander und Rita Abrahamsen (Hg.): Routledge handbook of private security studies. London, New York: Routledge (Routledge handbooks), S. 168–176.

Newman, Lily Hay (2019): What Israel's Strike on Hamas Hackers Means For Cyberwar. Hg. v. Wired. Online verfügbar unter https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/, zuletzt aktualisiert am 06.05.2019, zuletzt geprüft am 13.10.2021.

Nichols, Michelle (2020): U.S. withdrawal from WHO over claims of China influence to take effect July 2021: U.N. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-health-coronavirus-trump-who-idUSKBN2482YZ, zuletzt aktualisiert am 07.07.2020, zuletzt geprüft am 06.10.2021.

Noack, Rick (2018): How a Dutch intelligence agency secretly hacked into the Kremlin's most notorious hacking group. Hg. v. Independent. Online verfügbar unter https://www.independent.co.uk/news/world/europe/netherlands-dutch-russia-kremlin-united-states-robert-mueller-intelligence-agencies-cozy-bear-aivd-a8181046.html, zuletzt aktualisiert am 27.01.2018.

Noble, Ben; Schulmann, Ekaterina (2021): Myth 15: »It's All About Putin – Russia is a manually run, centralized autocracy«. Hg. v. Chatham House. Online verfügbar unter https://www.chathamhouse.org/2021/05/myths-and-misconceptions-debate-russia/myth-15-its-all-about-putin-russia-manually-run, zuletzt aktualisiert am 13.05.2021, zuletzt geprüft am 18.05.2021.

Nossek, Hillel; Limor, Yehiel (2001): Fifty Years In A« Marriage Of Convenience«: News Media And Military Censorship In Israel. In: Communication Law & Policy 6 (1), S. 1–35.

Novetta (2014): Operation SMN: Axiom Threat Actor Group Report. Hg. v. Novetta. Online verfügbar unter http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf.

Novetta (2016): Operation Blockbuster. Unraveling the Long Thread of the Sony Attack. Hg. v. Novetta. Online verfügbar unter https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf.

Nye, Joseph S. (2011): Nuclear lessons for cyber security? In: Strategic Studies Quarterly 5 (4), S. 18–38.

Nye, Joseph S. (2017): Deterrence and Dissuasion in Cyberspace. In: International Security 41 (3), S. 44–71. DOI: 10.1162/ISEC_a_00266.

Nye, Joseph S. (2018): Protecting Democracy in an Era of Cyber Information War. Hg. v. Hoover Institution (Fall Series, Issue 318). Online verfügbar unter https://www.hoover.org/research/protecting-democracy-era-cyber-information-war, zuletzt aktualisiert am 13.11.2018, zuletzt geprüft am 12.05.2020.

O'Hara, Terence (2005): In-Q-Tel, CIA's Venture Arm, Invests in Secrets. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/wp-dyn/content/article/2005/08/14/AR2005081401108.html, zuletzt aktualisiert am 02.08.2016, zuletzt geprüft am 12.08.2021.

Obama, Barack (2011): Remarks By President Obama to the Australian Parliament. Hg. v. The White House. Online verfügbar unter https://eu.usatoday.com/story/news/world/2014/04/28/obama-philippines-china/8403801/, zuletzt aktualisiert am 17.11.2011, zuletzt geprüft am 02.08.2021.

O'Brien, Kevin J.; Li, Lianjiang (2000): Accommodating »Democracy« in a One-Party State: Introducing Village Elections in China. In: The China Quarterly 162, S. 465–489. DOI: 10.1017/s0305741000008213.

ODNI (2017): Background to »Assessing Russian Activities and Intentions in Recent US Elections«: The Analytic Process and Cyber Incident Attribution. Hg. v. Office of the Director of National Intelligence. Online verfügbar unter https://www.dni.gov/files/documents/ICA_2017_01.pdf, zuletzt aktualisiert am 06.01.2017, zuletzt geprüft am 19.04.2021.

ODNI (2018): A Guide to Cyber Attribution. Hg. v. Office of the Director of National Intelligence. Online verfügbar unter https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf, zuletzt aktualisiert am 14.09.2018.

Olson, Parmy (2014): The Largest Cyber Attack In History Has Been Hitting Hong Kong Sites. Hg. v. Forbes. Online verfügbar unter https://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/?sh=722c95a838f6, zuletzt aktualisiert am 20.11.2014, zuletzt geprüft am 30.07.2021.

Oneal, John R.; Russet, Bruce M. (1997): The classical liberals were right: Democracy, interdependence, and conflict, 1950–1985. In: Int Stud Q 41 (2), S. 267–293.

Oneal, John R.; Russett, Bruce; Berbaum, Michael L. (2003): Causes of peace: Democracy, interdependence, and international organizations, 1885–1992. In: Int Stud Q 47 (3), S. 371–393.

O'Neill, Patrick Howell (2017): Report: Russian arrests allegedly tied to passing hacking information to U.S. Hg. v. Cyberscoop. Online verfügbar unter https://www.cyberscoop.com/russia-fsb-arrests-king-servers-threatconnect/, zuletzt aktualisiert am 26.01.2017, zuletzt geprüft am 06.05.2021.

O’Neill, Patrick Howell (2020a): Inside NSO, Israel’s billion-dollar spyware giant. Hg. v. MIT Technology Review. Online verfügbar unter https://www.technologyreview.com/2020/08/19/1006458/nso-spyware-controversy-pegasus-human-rights/, zuletzt aktualisiert am 19.08.2020, zuletzt geprüft am 03.01.2022.

O’Neill, Patrick Howell (2020b): The NSA found a dangerous flaw in Windows and told Microsoft to fix it. Hg. v. MIT Technology Review. Online verfügbar unter https://www.technologyreview.com/2020/01/14/75069/the-nsa-found-a-dangerous-flaw-in-windows-and-told-microsoft-to-fix-it/, zuletzt aktualisiert am 15.01.2020, zuletzt geprüft am 01.10.2021.

O’Neill, Patrick Howell (2021): Google’s top security teams unilaterally shut down a counterterrorism operation. Hg. v. MIT Technology Review. Online verfügbar unter https://www.technologyreview.com/2021/03/26/1021318/google-security-shut-down-counter-terrorist-us-ally/, zuletzt aktualisiert am 26.03.2021, zuletzt geprüft am 20.08.2021.

Orbach, Meir (2020): Microsoft in Negotiations to Acquire Israeli Cybersecurity Company CyberX. Hg. v. Calcalist. Online verfügbar unter https://www.calcalistech.com/ctech/articles/0,7340,L-3817591,00.html, zuletzt aktualisiert am 05.05.2020, zuletzt geprüft am 11.10.2021.

Oren, Ido (1995): The Subjectivity of the »Democratic« Peace: Changing U.S. Perceptions of Imperial Germany. In: International Security 20 (2), S. 147–184. DOI: 10.2307/2539232.

Orye, Erwin; Maennel, Olaf M. (2019): Recommendations for Enhancing the Results of Cyber Effects. In: Tomáš Minárik, Siim Alatalu, Stefano Biondi, Massimiliano Signoretti, Ihsan Tolga und Gabor Visky (Hg.): 2019 11th International Conference on Cyber Conflict (CyCon). Tallinn, Estonia: IEEE, S. 1–19.

Osborne, Charlie (2020): Microsoft has the highest rate of zero-days detected in the wild, but not all is as it seems. Hg. v. The Daily Swig. Online verfügbar unter https://portswigger.net/daily-swig/microsoft-has-the-highest-rate-of-zero-days-detected-in-the-wild-but-not-all-is-as-it-seems, zuletzt aktualisiert am 31.07.2020, zuletzt geprüft am 11.06.2021.

Østensen, Åse Gilje; Bukkvoll, Tor (2018): Russian Use of Private Military and Security Companies-the implications for European and Norwegian Security. In: FFI-rapport 18, S. 1–49. Online verfügbar unter https://open.cmi.no/cmi-xmlui/bitstream/handle/11250/2564170/Russian%20Use%20of%20Private%20Military%20and%20Security%20Companies%20-%20the%20implications%20for%20European%20and%20Norwegian%20Security?sequence=1, zuletzt geprüft am 19.05.2020.

Ottis, Rain (2010): Proactive Defence Tactics Against On-Line Cyber Militia. In: Joseph Demergis (Hg.): Proceedings of the 9th European Conference on Information Warfare and Security. Proceedings of the 9th European Conference on Information Warfare and Security. Thessaloniki, 01.-02. Juli 2010. Reading: Academic Publishing Limited, S. 233–237.

Owen, John M. (1994): How Liberalism Produces Democratic Peace. In: International Security 19 (2), S. 87. DOI: 10.2307/2539197.

Page, Carly (2021): EU warns Russia over ›Ghostwriter‹ hacking ahead of German elections. Hg. v. Techcrunch. Online verfügbar unter https://techcrunch.com/2021

/09/24/european-council-russia-ghostwriter/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAADuClHZMVk9Lh5I9ZZ0F4hfr36d00c4fujTkb_ZJw1Lt9qcb2uphqRQkSk-I61cqEX4M8uOak5sxPZQrOPBf4ZdR8JbZOIlIPz7bsLq5vxpAjdKVKHVRJDOQSR9dprxGoQAxe1MkIxOgHx7OQ_XR10qQjFCu2szmXCt0xiM5Z48u, zuletzt aktualisiert am 24.09.2021, zuletzt geprüft am 10.02.2022.

Palm, Philip M.; Schulz, Daniel F. (2011): Die Beteiligung am Irak-Krieg – eine innenpolitische Frage? In: Markus M. Müller (Hg.): Casebook internationale Politik. 1. Aufl. Wiesbaden: VS Verl. für Sozialwiss (Lehrbuch), S. 64–87.

Palo Alto Networks (2021): Management. Hg. v. Palo Alto Networks. Online verfügbar unter https://www.paloaltonetworks.com/about-us/management, zuletzt geprüft am 11.10.2021.

Park, Donghui; Walstrom, Michael (2017): Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks – The Henry M. Jackson School of International Studies. Hg. v. The Henry M. Jackson School of International Studies. Online verfügbar unter https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/, zuletzt aktualisiert am 11.10.2017, zuletzt geprüft am 18.04.2021.

Parker, Ned; Landay, Jonathan; Walcott, John (2017): Putin-linked think tank drew up plan to sway 2016 US election – documents. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-usa-russia-election-exclusive/putin-linked-think-tank-drew-up-plan-to-sway-2016-us-election-documents-idUSKBN17L2N3, zuletzt aktualisiert am 19.04.2017, zuletzt geprüft am 14.04.2021.

Paul, Kari (2021): SolarWinds hack was work of ›at least 1,000 engineers‹, tech executives tell Senate. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/technology/2021/feb/23/solarwinds-hack-senate-hearing-microsoft, zuletzt aktualisiert am 24.02.2021, zuletzt geprüft am 12.05.2021.

Paul, Michael (2018): Chinas nukleare Abschreckung: Ursachen, Mittel und Folgen der Stationierung chinesischer Nuklearwaffen auf Unterseebooten. Hg. v. Stiftung Wissenschaft Und Politik. Berlin (SWP-Studie, 17). Online verfügbar unter https://www.ssoar.info/ssoar/handle/document/59759, zuletzt geprüft am 31.07.2021.

Pavur, James (2021): Securing new space: on satellite cyber-security. Hg. v. University of Oxford (A thesis submitted for the degree of Doctor of Philosophy). Online verfügbar unter https://ora.ox.ac.uk/objects/uuid:11e1b32a-8117-46b1-a0ce-9c485221d112, zuletzt geprüft am 23.11.2021.

Perez, Evan (2016): U.S. official blames Russia for power grid attack in Ukraine – CNNPolitics. Hg. v. CNN. Online verfügbar unter https://edition.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/index.html, zuletzt aktualisiert am 12.02.2016, zuletzt geprüft am 29.09.2021.

Peri, Yoram (1981): Political-Military Partnership in Israel. In: International Political Science Review 2 (3), S. 303–315. Online verfügbar unter http://www.jstor.org/stable/1601065.

Perlroth, Nicole (2012): In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2012/10/24

/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html, zuletzt aktualisiert am 23.10.2012.

Perlroth, Nicole (2013): Chinese Hackers Infiltrate New York Times Computers. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html, zuletzt aktualisiert am 30.01.2013, zuletzt geprüft am 02.08.2021.

Perlroth, Nicole (2021): This Is How They Tell Me the World Ends. London: Bloomsbury Publishing.

Pernik, Piret (2018): The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine. In: Nicu Popescu und Stanislav Secrieru (Hg.): Hacks, Leaks and Disruptions: Russian Cyber Strategies. Paris (Chaillot Papers, 148), S. 53–64.

Peters, Allison (2019): Russia and China Are Trying to Set the U.N.‹s Rules on Cybercrime. Hg. v. Foreign Policy. Online verfügbar unter https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/, zuletzt aktualisiert am 16.09.2019.

Peters, Michael A. (2017): The Chinese Dream: Xi Jinping thought on Socialism with Chinese characteristics for a new era. In: Educational Philosophy and Theory 49 (14), S. 1299–1304. DOI: 10.1080/00131857.2017.1407578.

Peterson, Demosthenes James (2005): Russia and the information revolution. Santa Monica, Calif. (Rand Corporation monograph series, MG-422-CC).

Piiparinen, Anni (2016): China's Secret Weapon in the South China Sea: Cyber Attacks. Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/, zuletzt aktualisiert am 22.06.2016, zuletzt geprüft am 23.06.2021.

Pillar, Paul R. (2011): Intelligence and US foreign policy: Iraq, 9/11, and misguided reform: Columbia University Press.

Plan, Fred; Fraser, Nalani; O'Leary Jacqueline; Cannon, Vincent; Read, Ben (2019): APT40: Examining a China-Nexus Espionage Actor. Hg. v. FireEye. Online verfügbar unter https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html, zuletzt aktualisiert am 04.09.2019, zuletzt geprüft am 01.07.2021.

Poitras, Laura; Rosenbach, Marcel; Stark, Holger (2013): ›Follow the Money‹: NSA Monitors Financial World. Hg. v. Der Spiegel. Online verfügbar unter https://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html, zuletzt aktualisiert am 16.09.2013, zuletzt geprüft am 26.08.2021.

Polaski, Sandra; Dollar, David (2020): How have Trump's trade wars affected Rust Belt jobs? Hg. v. Brookings. Online verfügbar unter https://www.brookings.edu/podcast-episode/how-have-trumps-trade-wars-affected-rust-belt-jobs/, zuletzt aktualisiert am 19.10.2020, zuletzt geprüft am 06.10.2021.

Pouliot, Vincent (2014): Setting Status in Stone: The Negotiation of International Institutional Privileges. In: T. V. Paul, Deborah Welch Larson und William C. Wohlforth (Hg.): Status in World Politics: Cambridge University Press, S. 192–218.

Pouliot, Vincent (2016): International Pecking Orders. The Politics and Practice of Multilateral Diplomacy: Cambridge University Press.

Pozen, David E. (2013): THE LEAKY LEVIATHAN: WHY THE GOVERNMENT CONDEMNS AND CONDONES UNLAWFUL DISCLOSURES OF INFORMATION. In: Harvard law review 127 (2), S. 512–635. Online verfügbar unter http://www.jstor.org/stable/23742018.

Poznansky, Michael; Perkoski, Evan (2018): Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution. In: Journal of Global Security Studies 3 (4), S. 402–416.

PRC Embassy Iraq (2017): Speech By President Xi Jinping At the United Nations Office at Geneva. Hg. v. Embassy of the People's Republic of China in the Republic of Iraq. Online verfügbar unter http://iq.chineseembassy.org/eng/zygx/t1432869.htm, zuletzt aktualisiert am 23.01.2017, zuletzt geprüft am 04.08.2021.

PRC Embassy Philippines (2016): Archaeological Findings Prove That Chinese People Are Real Owner of South China Sea Islands. Hg. v. Embassy of the People's Republic of China in the Rebublic of the Philippines. Online verfügbar unter http://ph.china-embassy.org/eng/sgdt/t1372445.htm, zuletzt aktualisiert am 15.06.2016, zuletzt geprüft am 02.08.2021.

Precht, Henry (1988): Ayatollah realpolitik. In: Foreign Policy (70), S. 109–128.

Proofpoint (2017): Leviathan: Espionage actor spearphishes maritime and defense targets | Proofpoint US. Hg. v. Proofpoint. Online verfügbar unter https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets, zuletzt aktualisiert am 27.01.2019, zuletzt geprüft am 01.07.2021.

Protasov, Vitaly (2010): EU-Russia Gas Relations: a View From Both Sides. Hg. v. International Association for Energy Economics. Online verfügbar unter https://www.iaee.org/en/publications/newsletterdl.aspx?id=115#:~:text=Dependence%20on%20Russian%20gas%20is,from%20Russia%20in%20prior%20years., zuletzt geprüft am 12.05.2021.

Ptak, Alicija; Pawlak, Justyna (2021): Polish trial begins in Huawei-linked China espionage case. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/world/china/polish-trial-begins-huawei-linked-china-espionage-case-2021-05-31/, zuletzt aktualisiert am 01.06.2021, zuletzt geprüft am 05.07.2021.

Putnam, Robert D. (1988): Diplomacy and domestic politics: the logic of two-level games. In: International Organization, S. 427–460.

Putnam, Tonya L.; Elliott, David D. (2001): International Responses to cyber crime. In: Transnational Dimension of Cyber Crime and Terrorism, S. 35–66.

Radio Free Europe (2017): Putin Compares Hackers To ›Artists,‹ Says They Could Target Russia's Critics For ›Patriotic‹ Reasons. Hg. v. Radio Free Europe. Online verfügbar unter https://www.rferl.org/a/russia-putin-patriotic-hackers-target-critics-not-state/28522639.html, zuletzt aktualisiert am 01.06.2017, zuletzt geprüft am 20.05.2021.

Rakuszitzky, Moritz; Romein, Daniel; Dobrokhotov, Roman (2018): MH17 – Russian GRU Commander ›Orion‹ Identified as Oleg Ivannikov. Hg. v. Bellingcat. Online verfügbar unter https://www.bellingcat.com/news/uk-and-europe/2018/05/25/mh17-russian-gru-commander-orion-identified-oleg-ivannikov/, zuletzt aktualisiert am 05.09.2018, zuletzt geprüft am 12.05.2021.

Ramadhani, Eryan (2019): Is Assertiveness Paying the Bill? China's Domestic Audience Costs in the South China Sea Disputes. In: Journal of Asian Security and International Affairs 6 (1), S. 30–54.

Rathbun, Brian C. (2010): Is anybody not an (international relations) liberal? In: Security Studies 19 (1), S. 2–25.

Raud, Mikk (2015): China and cyber: attitude, strategies, organisation. Hg. v. NATO CCD COE. Tallinn. Online verfügbar unter https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf, zuletzt aktualisiert am 2016, zuletzt geprüft am 10.01.2021.

Rauta, Vladimir (2020): Proxy Warfare and the Future of Conflict: Take Two. In: The RUSI Journal 165 (2), S. 1–10. DOI: 10.1080/03071847.2020.1736437.

Rauta, Vladimir (2021): ›Proxy War‹-A Reconceptualisation. In: Civil Wars 23 (1), S. 1–24.

Ray, Siladitya (2020): Report: CIA Conducted Cyber Attacks Against Iran, Russia After Secret Trump Order In 2018. Hg. v. Forbes. Online verfügbar unter https://www.forbes.com/sites/siladityaray/2020/07/15/report-cia-conducted-cyber-attacks-against-iran-russia-after-secret-trump-order-in-2018/?sh=22006c194600, zuletzt aktualisiert am 15.07.2020, zuletzt geprüft am 06.10.2021.

Recorded Future (2017): Recorded Future Launches Threat Research Arm to Enhance Threat Intelligence Offering. Hg. v. Recorded Future. Online verfügbar unter https://www.prnewswire.com/news-releases/recorded-future-launches-threat-research-arm-to-enhance-threat-intelligence-offering-300454937.html, zuletzt aktualisiert am 10.05.2017, zuletzt geprüft am 12.08.2021.

Reed, John (2015): Unit 8200: Israel's cyber spy agency. Hg. v. Financial Times. Online verfügbar unter https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c, zuletzt aktualisiert am 10.07.2015, zuletzt geprüft am 02.01.2022.

Reinhold, Thomas; Reuter, Christian (2021): Towards a Cyber Weapons Assessment Model -Assessment of the Technical Features of Malicious Software. In: IEEE Transactions on Technology and Society, S. 1. DOI: 10.1109/TTS. 2021.3131817.

Reuters (2011): Russia's Medvedev fires deputy FSB security chief. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/russia-medvedev-fsb-idUSLDE71K1NH20110221, zuletzt aktualisiert am 21.02.2011, zuletzt geprüft am 12.05.2021.

Reuters (2013): Iran ups cyber attacks on Israeli computers: Netanyahu. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-israel-iran-cyber-idUSBRE95808H20130609, zuletzt aktualisiert am 09.06.2013, zuletzt geprüft am 07.10.2021.

Reuters (2020a): ›There will be dad and mum‹: Putin rules out Russia legalizing gay marriage. Hg. v. NBC News. Online verfügbar unter https://www.nbcnews.com/feature/nbc-out/there-will-be-dad-mum-putin-rules-out-russia-legalizing-n1136936, zuletzt aktualisiert am 14.02.2020, zuletzt geprüft am 05.05.2021.

Reuters (2020b): Timeline: Key dates in Hong Kong's anti-government protests. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-hongkong-protests-timeline-idUSKBN23608O, zuletzt aktualisiert am 30.05.2020, zuletzt geprüft am 30.07.2021.

Reuters (2020c): Timeline: Key dates in the U.S.-China trade war. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-usa-trade-china-timeline-idUSKBN1ZE1AA, zuletzt aktualisiert am 15.01.2020, zuletzt geprüft am 01.10.2021.

Richter, Steffen (2013): Bo Xilai-Urteil: Xi Jinping gnadenlos. Hg. v. Die Zeit. Online verfügbar unter https://www.zeit.de/politik/ausland/2013-09/xi-jinping-bo-xilai-reformen?utm_referrer=https%3A%2F%2Fwww.google.com%2F, zuletzt aktualisiert am 23.09.2013, zuletzt geprüft am 25.07.2021.

Rid, Thomas (2013): Cyberwar and Peace: Hacking Can Reduce Real-World Violence. In: Foreign Affairs 92 (6), S. 77–87.

Rid, Thomas; Buchanan, Ben (2015): Attributing Cyber Attacks. In: Journal of Strategic Studies 38 (1–2), S. 4–37. DOI: 10.1080/01402390.2014.977382.

Rivera, David W.; Rivera, Sharon Werning (2018): The Militarization of the Russian Elite under Putin. In: Problems of Post-Communism 65 (4), S. 221–232. DOI: 10.1080/10758216.2017.1295812.

Rivera, Jason (2015): Achieving cyberdeterrence and the ability of small states to hold large states at risk. In: M. Maybaum (Hg.): 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace (CyCon). 26–29 May 2015, Tallinn, Estonia. Piscataway, NJ: IEEE, S. 7–24.

Roberts, Samuel J. (2019): Party and policy in Israel: The battle between hawks and doves: Routledge.

Robinson, Glenn E. (2020): The death of the two-state solution. Israel, the Palestinians, and the Arab world in the age of Netanyahu. In: Robert O. Freedman (Hg.): Israel Under Netanyahu: Domestic Politics and Foreign Policy: Routledge.

Rød, Espen Geelmuyden; Weidmann, Nils B. (2015): Empowering activists or autocrats? The Internet in authoritarian regimes. In: Journal of Peace Research 52 (3), S. 338–351.

Röhl, Klaus-Heiner (2016): Unternehmensgründungen: Mehr innovative Startups durch einen Kulturwandel für Entrepreneurship? Hg. v. Institut für deutsche Wirtschaft Köln. Online verfügbar unter https://www.iwkoeln.de/fileadmin/publikationen/2016/262911/Unternehmensgruendungen_IW_policy_paper.pdf, zuletzt aktualisiert am 28.01.2016, zuletzt geprüft am 26.10.2021.

Rohlfing, Ingo (2014): Comparative Hypothesis Testing Via Process Tracing. In: Sociological Methods & Research 43 (4), S. 606–642. DOI: 10.1177/0049124113503142.

Romagna, Marco; van den Hout, Niek Jan (2017): Hacktivism and website defacement: motivations, capabilities and potential threats. Virus Bulletin Conference. Madrid. Online verfügbar unter https://www.virusbulletin.com/conference/vb2017/abstracts/hacktivism-and-website-defacement-motivations-capabilities-and-potential-threats, zuletzt aktualisiert am 2017, zuletzt geprüft am 11.06.2020.

Romanosky, Sasha (2017): Private-Sector Attribution of Cyber Attacks: A Growing Concern for the U.S. Government? Hg. v. Lawfare. Online verfügbar unter https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government, zuletzt aktualisiert am 21.12.2017, zuletzt geprüft am 13.07.2020.

Romanosky, Sasha; Boudreaux, Benjamin (2021): Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government. In: Interna-

tional Journal of Intelligence and CounterIntelligence 34 (3), S. 463–493. DOI: 10.1080/08850607.2020.1783877.

Roncone, Gabriella; Wahlstrom, Alden; Revelli, Alice; Mainor, David; Riddell, Sam; Read, Ben (2021): UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests | Mandiant. Hg. v. MANDIANT. Online verfügbar unter https://www.mandiant.com/resources/unc1151-linked-to-belarus-government, zuletzt aktualisiert am 16.11.2021, zuletzt geprüft am 10.02.2022.

Rondeaux, Candace (2019): Decoding the Wagner group: Analyzing the role of private military security contractors in Russian proxy warfare. Hg. v. Center on the Future of War. Arizona State University. Online verfügbar unter https://www.ohchr.org/Documents/issues/Mercenaries/WG/OtherStakeholders/candace-rondeux-submission-1.pdf.

Rosenbach, Eric; Chong, Shu Min (2019): Governing Cyberspace: State Control vs. The Multistakeholder Model. Hg. v. Belfer Center for Science and International Affairs. Online verfügbar unter https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model, zuletzt geprüft am 15.12.2022.

Ross, Ingrid (2005): Hijacking of the President? Die Neokonservativen und die Entscheidung zum Irakkrieg 2003. Göttingen, Berlin: Niedersächsische Staats- und Universitätsbibliothek; John-F.-Kennedy-Institut für Nordamerikastudien (Working paper/ John-F.-Kennedy-Institut für Nordamerikastudien, 134). Online verfügbar unter http://webdoc.sub.gwdg.de/ebook/serien/p/jfk/workingpaper134.pdf.

Roth, Andrew (2019): Russia's great firewall: is it meant to keep information in – or out? Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/technology/2019/apr/28/russia-great-firewall-sovereign-internet-bill-keeping-information-in-or-out, zuletzt aktualisiert am 28.04.2019.

Roth, Andrew (2021): Ukraine still outgunned as Russia prepares for larger conflict. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2021/apr/14/ukraine-still-outgunned-as-russia-prepares-for-larger-conflict, zuletzt aktualisiert am 14.04.2021, zuletzt geprüft am 18.05.2021.

Rousseau, David L.; Gelpi, Christopher; Reiter, Dan; Huth, Paul K. (1996): Assessing the dyadic nature of the democratic peace, 1918–88. In: Am Polit Sci Rev 90 (3), S. 512–533.

Rugge, Fabio (Hg.) (2018): Confronting an »axis of cyber«? China, Iran, North Korea, Russia in cyberspace. First edition. Milano: ISPI Ledizioni LediPublishing. Online verfügbar unter https://www.doabooks.org/doab?func=fulltext&uiLanguage=en&rid=29716.

Russett, Bruce (1994): Grasping the democratic peace: Principles for a post-Cold War world: Princeton University Press.

Rutland, Peter (2018): The Political Elite in Post-Soviet Russia. In: The Palgrave Handbook of Political Elites: Springer, S. 273–294.

Saalbach, Klaus-Peter (2019): Attribution of Cyber Attacks. In: Christian Reuter (Hg.): Information Technology for Peace and Security. Wiesbaden: Springer Vieweg, S. 279–303.

Saalman, Lora (2017): New domains of crossover and concern in cyberspace. Hg. v. Stockholm International Peace Research Institute. Online verfügbar unter https:/

/www.sipri.org/commentary/topical-backgrounder/2017/new-domains-crossover-and-concern-cyberspace, zuletzt aktualisiert am 26.07.2017, zuletzt geprüft am 11.01.2022.

Sadeh, Shuki (2021): Israeli military vs. NSO: The battle for talent is getting dark. Hg. v. Haaretz. Online verfügbar unter https://www.haaretz.com/israel-news/tech-news/idf-vs-nso-8200-battle-israel-cyber-talent-getting-dark-1.9929433, zuletzt aktualisiert am 29.06.2021, zuletzt geprüft am 02.01.2022.

Sakwa, Richard (2008): Putin and the Oligarchs. In: New Political Economy 13 (2), S. 185–191. DOI: 10.1080/13563460802018513.

Sakwa, Richard (2012): Party and power: between representation and mobilisation in contemporary Russia. In: East European Politics 28 (3), S. 310–327. DOI: 10.1080/21599165.2012.683784.

Sambaluk, Nick (2019): Conflict in the 21st Century. The Impact of Cyber Warfare, Social Media, and Technology. Santa Barbara, CA, Denver, CO: ABC-CLIO.

Sanchez, Julian (2020): No, The Presidential Election Was Not Rigged by Hacked Voting Machines. Hg. v. Cato Institute. Online verfügbar unter https://www.cato.org/blog/no-presidential-election-was-not-rigged-hacked-voting-machines, zuletzt aktualisiert am 13.11.2020, zuletzt geprüft am 05.05.2021.

Sanger, David E.; Perlroth, Nicole (2013): China's Army Is Seen as Tied to Hacking Against U.S. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html, zuletzt aktualisiert am 18.02.2013, zuletzt geprüft am 02.07.2021.

Sanger, David E.; Schmall, Emily (2021): China Appears to Warn India: Push Too Hard and the Lights Could Go Out. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html, zuletzt aktualisiert am 28.02.2021, zuletzt geprüft am 04.08.2021.

Sartori, Giovanni (1970): Concept misformation in comparative politics. In: American Political Science Review 64 (4), S. 1033–1053.

Satter, David (2003): Darkness at dawn: The rise of the Russian criminal state: Yale University Press.

Satter, Raphael (2020): Exclusive-Suspected Chinese hackers stole camera footage from African Union – memo. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/idUSKBN28Q1DB, zuletzt aktualisiert am 16.12.2020, zuletzt geprüft am 23.06.2021.

Schake, Kori (2020): The Military and the Constitution Under Trump. In: Survival 62 (4), S. 31–38. DOI: 10.1080/00396338.2020.1792096.

Schambra, William (2009): Obama and the Policy Approach. Hg. v. National Affairs. Online verfügbar unter https://www.nationalaffairs.com/publications/detail/obama-and-the-policy-approach, zuletzt geprüft am 02.09.2021.

Schelling, Thomas C. (1960): The Strategy of Conflict. Cambridge, Massachusetts: Harvard University Press.

Schepp, Matthias (2013): Bürgermeisterwahl in Moskau: Putin – der große Verlierer. Hg. v. Der Spiegel. Online verfügbar unter https://www.spiegel.de/politik/ausland/buergermeisterwahl-in-moskau-verlierer-putin-a-921104.html, zuletzt aktualisiert am 09.09.2013, zuletzt geprüft am 29.04.2021.

Schiermeier, Quirin (2014): Putin's Russia divides and enrages scientists. In: Nature 516 (7531), S. 298–299. DOI: 10.1038/516298a.

Schimmelfennig, Frank (2013): Internationale Politik. 3., aktualisierte Aufl. Paderborn: Schöningh (UTB, 3107 : Politikwissenschaft).

Schmidt, Michael S.; Sanger, David E.; Perlroth, Nicole (2014): Chinese Hackers Pursue Key Data on U.S. Workers. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html, zuletzt aktualisiert am 09.07.2014, zuletzt geprüft am 27.09.2021.

Schmitt, Michael N. (2015): The law of cyber targeting. In: Naval War College Review 68 (2), S. 10–29. Online verfügbar unter https://www.jstor.org/stable/26397834.

Schmitt, Michael N.; Vihul, Liis (2014): Proxy Wars in Cyberspace: The Evolving International Law of Attribution. In: Fletcher Security Review 1, S. 53.

Schneier, Bruce (2014): Essays: Did North Korea Really Attack Sony? – Schneier on Security. Hg. v. Schneier on Security. Online verfügbar unter https://www.schneier.com/essays/archives/2014/12/did_north_korea_real.html, zuletzt aktualisiert am 22.12.2014, zuletzt geprüft am 11.08.2021.

Schreyer, Söhnke (2017): Geteilte Herrschaft: Obama, die parteipolitische Polarisierung und der Kongress. In: Z Außen Sicherheitspolit 10 (S2), S. 25–38. DOI: 10.1007/s12399-017-0617-1.

Schröder, Hans-Henning (2018): Russland in der Ära Jelzin. Hg. v. Bundeszentrale für Politische Bildung. Online verfügbar unter https://www.bpb.de/internationales/europa/russland/47924/russland-in-der-aera-jelzin-1992-1999?p=2, zuletzt aktualisiert am 11.06.2018, zuletzt geprüft am 28.04.2021.

Schubarth, Cromwell (2021): What CrowdStrike CEO George Kurtz says about the controversy that got Donald Trump so angry. Hg. v. Silicon Valley Business Journal. Online verfügbar unter https://www.bizjournals.com/sanjose/news/2021/06/25/middle-market-75-crowdstrike-ukraine.html, zuletzt aktualisiert am 25.06.2021, zuletzt geprüft am 20.08.2021.

Schulze, Matthias (2019): Quo Vadis Cyber Arms Control? – A Sketch of an International Vulnerability Equities Process and a 0-Day Emissions Trading Regime. In: Christian Reuter, Jürgen Altmann, Malte Göttsche und Mirko Himmel (Hg.): Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research. Science Peace Security '19. Darmstadt, 25.-27.9.2019. Darmstadt: TUprints, S. 24–40.

Schulze, Matthias (2020): The State of Cyber Arms Control. An International Vulnerabilities Equities Process as the Way to go Forward? In: S&F Sicherheit und Frieden 38 (1), S. 17–21.

Schulzke, Marcus (2018): The politics of attributing blame for cyberattacks and the costs of uncertainty. In: Perspectives on Politics 16 (4), S. 954–968.

Schünemann, Wolf J. (2020): Cybersicherheit. In: Tanja Klenk, Frank Nullmeier und Göttrik Wewer (Hg.): Handbuch Digitalisierung in Staat und Verwaltung. Wiesbaden: Springer Fachmedien Wiesbaden, S. 199–208.

Schwartz, Mathew J. (2017): French Officials Detail ›Fancy Bear‹ Hack of TV5Monde. Hg. v. Bankinfo Security. Online verfügbar unter https://www.bankinfosecurity.com

/french-officials-detail-fancy-bear-hack-tv5monde-a-9983, zuletzt aktualisiert am 12.06.2017, zuletzt geprüft am 19.04.2021.

Scobell, Andrew (2000): Chinese Army Building in the Era of Jiang Zemin. Carlisle: Strategic Studies Institute, U.S. Army War College.

Scott-Railton, John; Marczak, Bill; Anstis, Siena; Razzak, Bahr Abdul; Crete-Nishihata, Masashi; Deibert, Ron (2019): Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware. Hg. v. The Citizen Lab. Online verfügbar unter https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/, zuletzt aktualisiert am 20.03.2019, zuletzt geprüft am 26.10.2021.

Scott-Railton, John; Marczak, Bill; Razzak, Bahr Abdul; Crete-Nishihata, Masashi; Deibert, Ron (2017): Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware – The Citizen Lab. Hg. v. The Citizen Lab. Online verfügbar unter https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/, zuletzt aktualisiert am 19.06.2017, zuletzt geprüft am 26.10.2021.

Seals, Tara (2018): UK Launches Offensive Cyber-Weapons Against Islamic State. Hg. v. Infosecurity Magazine. Online verfügbar unter https://www.infosecurity-magazine.com/news/uk-launches-offensive-cyberweapons/, zuletzt aktualisiert am 12.04.2018.

Securelist (2013): Winnti. More than just a game. Hg. v. Kaspersky. Online verfügbar unter https://securelist.com/winnti-more-than-just-a-game/37029/, zuletzt aktualisiert am 11.04.2013, zuletzt geprüft am 25.06.2021.

Security Joes (2021): In the Media. News. Hg. v. Security Joes. Online verfügbar unter https://www.securityjoes.com/news, zuletzt aktualisiert am 26.09.2021, zuletzt geprüft am 06.01.2022.

Segal, Adam (2016): The U.S.-China Cyber Espionage Deal One Year Later. Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later, zuletzt aktualisiert am 28.09.2016, zuletzt geprüft am 04.08.2021.

Segal, Adam (2018): Cyber Week in Review: January 26, 2018. Hg. v. Council on Foreign Relations. Online verfügbar unter https://www.cfr.org/blog/cyber-week-review-january-26-2018, zuletzt aktualisiert am 26.01.2018, zuletzt geprüft am 20.08.2021.

Seybolt, Taylor B. (2007): Humanitarian military intervention: the conditions for success and failure: SIPRI Publication.

Shachtman, Noah (2010): Exclusive: Google, CIA Invest in ›Future‹ of Web Monitoring. Hg. v. Wired. Online verfügbar unter https://www.wired.com/2010/07/exclusive-google-cia/, zuletzt aktualisiert am 29.07.2010, zuletzt geprüft am 12.08.2021.

Shackelford, Scott J.; Sulmeyer, Michael; Deckard, Amanda N. Craig; Buchanan, Ben; Micic, Brian (2017): From Russia with Love: Understanding the Russian Cyber Threat to US Critical Infrastructure and What to Do about It. In: Nebraska Law Review 96 (2), S. 320–338.

Shafy, Samiha (2022): Sturm auf das Kapitol: Nach dem Sturm. Hg. v. Die Zeit. Online verfügbar unter https://www.zeit.de/2022/02/kapitol-sturm-donald-trump-anhaenger, zuletzt aktualisiert am 06.01.2022, zuletzt geprüft am 18.01.2022.

Shah, Anup (2004): The Bush Doctrine of Pre-emptive Strikes; A Global Pax Americana. Hg. v. Global Issues. Online verfügbar unter https://www.globalissues.org/article/4

50/the-bush-doctrine-of-pre-emptive-strikes-a-global-pax-americana, zuletzt aktualisiert am 24.04.2004, zuletzt geprüft am 01.09.2021.
Shamir, Eli (2005): Computer Science and Technology in Israel 1950–1980. Hg. v. Rutherford Journal. Online verfügbar unter http://rutherfordjournal.org/article030111.html, zuletzt geprüft am 21.10.2021.
Shanghai Cooperation Organization (2009): Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security, 16.06.2009. Online verfügbar unter https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/SCO-090616-IISAgreement.pdf.
Sherstobitoff, Ryan; Malhotra, Asheer (2018): ›Operation Oceansalt‹ Attacks South Korea, U.S., and Canada With Source Code From Chinese Hacker Group. Hg. v. McAfee. Online verfügbar unter https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf#:~:text=McAfee%C2%AE%20Advanced%20Threat%20Research%20and%20Anti-Malware%20Operations%20teams,described%20this%20implant%20in%20any%20of%20our%20analyses., zuletzt aktualisiert am 18.10.2018, zuletzt geprüft am 02.07.2021.
Sheva, Arutz (2020): Cybersecurity: Israel Aerospace Industries collaborates with Mellanox Technologies. Hg. v. Arutz Sheva – Israel National News. Online verfügbar unter https://www.israelnationalnews.com/News/News.aspx/274641, zuletzt aktualisiert am 16.01.2020, zuletzt geprüft am 11.10.2021.
Shih, Gerry; Kuo, Lily (2021): Trump upsets decades of U.S. policy on Taiwan, leaving thorny questions for Biden. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/world/asia_pacific/trump-biden-taiwan-china/2021/01/13/1bbadee0-53c0-11eb-acc5-92d2819a1ccb_story.html, zuletzt aktualisiert am 13.01.2021, zuletzt geprüft am 02.08.2021.
Shirk, Susan (2017): Trump and China: Getting to yes with Beijing. In: Foreign Affairs 96, S. 20–27. Online verfügbar unter https://www.washingtonpost.com/world/asia_pacific/trump-biden-taiwan-china/2021/01/13/1bbadee0-53c0-11eb-acc5-92d2819a1ccb_story.html.
Shirk, Susan L. (2018): The Return to Personalistic Rule. In: Journal of Democracy 29 (2), S. 22–36. DOI: 10.1353/jod.2018.0022.
Shorrock, Tim (2016): 5 Corporations Now Dominate Our Privatized Intelligence Industry. Hg. v. The Nation. Online verfügbar unter https://www.thenation.com/article/archive/five-corporations-now-dominate-our-privatized-intelligence-industry/, zuletzt aktualisiert am 08.09.2016, zuletzt geprüft am 25.08.2021.
Sigholm, Johan (2013): Non-state actors in cyberspace operations. In: Journal of Military Studies 4 (1), S. 1–37.
Simon, Herbert A. (1972): Theories of bounded rationality. In: Decision and organization 1 (1), S. 161–176.
Simpson, Dwight J. (1970): Israel: A Garrison State. In: Current History 58 (341), S. 1–47. Online verfügbar unter http://www.jstor.org/stable/45314003.
Singhofen, Sven (2010): Kapitel 11 Terrorbekämpfung in Tschetschenien und im Nordkaukasus: Mission accomplished or failed? In: Jahrbuch Terrorismus 4, S. 193–214. Online verfügbar unter http://www.jstor.org/stable/24916942.

Smeets, Max (2020): U.S. cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection. In: Intelligence and National Security 35 (3), S. 444–453. DOI: 10.1080/02684527.2020.1729316.

Smeets, Max (2022, forthcoming): No Shortcuts. Why States Struggle to Develop a Military Cyber-Force. London: Hurst Publishers.

Smith, Noah (2021): Why is China smashing its tech industry? Hg. v. Noahpinion. Online verfügbar unter https://noahpinion.substack.com/p/why-is-china-smashing-its-tech-industry?token=eyJ1c2VyX2lkIjozMTU4OSwicG9zdF9pZCI6MzkxNjg0MDcsIl8iOiJxUEx3dSIsImlhdCI6MTYyNzQxNDM0NywiZXhwIjoxNjI3NDE3OTQ3LCJpc3MiOiJwdWItMzUzNDUiLCJzdWIiOiJwb3N0LXJlYWN0aW9uIn0.32h, zuletzt aktualisiert am 25.07.2021, zuletzt geprüft am 04.08.2021.

Snape, Holly; Wang, Weinan (2020): Finding a place for the Party: debunking the »party-state« and rethinking the state-society relationship in China's one-party system. In: Journal of Chinese Governance 5 (4), S. 477–502. DOI: 10.1080/23812346.2020.1796411.

Snowden, Edward (2019): Permanent record: Pan Macmillan.

Sobhani, Sohrab C. (1989): The pragmatic entente: Israeli-Iranian relations, 1948–1988. Dissertation. Georgetown University.

Soesanto, Stefan (2020): A one-sided Affair: Japan and the People's Republic of China in Cyberspace. In: CSS Cyberdefense Hotspot Analyses, S. 1–38. DOI: 10.3929/ethz-b-000389371.

Soesanto, Stefan (2021): The limits of like-mindedness in cyberspace. Hg. v. Elcano Royal Institute. Online verfügbar unter https://www.realinstitutoelcano.org/en/analyses/the-limits-of-like-mindedness-in-cyberspace/, zuletzt aktualisiert am 19.11.2021, zuletzt geprüft am 15.12.2022.

Soffer, Ari (2014): Report: IDF Foiled Massive Cyber-Attack on Israel. Hg. v. Israel National News. Online verfügbar unter https://www.israelnationalnews.com/News/News.aspx/184518#.U_, zuletzt aktualisiert am 28.08.2014, zuletzt geprüft am 07.10.2021.

Solomon, Lawrence (2012): Netanyahu's calculus. Hg. v. National Post. Online verfügbar unter https://nationalpost.com/opinion/lawrence-solomon-netanyahus-calculus, zuletzt aktualisiert am 19.08.2012, zuletzt geprüft am 03.01.2022.

Solomon, Shoshanna (2017): Israeli firm sees the spy agencies behind the sexy images. Hg. v. The Times of Israel. Online verfügbar unter https://www.timesofisrael.com/israel-firm-sees-the-spy-agencies-behind-the-sexy-images/, zuletzt aktualisiert am 28.08.2017, zuletzt geprüft am 11.10.2021.

Solomon, Shoshanna (2021): Alumni of 8200 unit win tender to boost women in R&D jobs. Hg. v. Times of Israel. Online verfügbar unter https://www.timesofisrael.com/alumni-of-8200-unit-win-tender-to-boost-women-in-rd-jobs/, zuletzt aktualisiert am 11.03.2021, zuletzt geprüft am 25.10.2021.

Sørli, Mirjam E.; Gleditsch, Nils Petter; Strand, Håvard (2005): Why is there so much conflict in the Middle East? In: Journal of Conflict Resolution 49 (1), S. 141–165.

Soschnikow, Andrej (2020): »Отключить интернет в небольшой стране«. Хакеры рассказали о новом кибероружии, заказанном ФСБ. Hg. v. BBC News Russia. Online verfügbar unter https://www.bbc.com/russian/news-51951933, zuletzt aktualisiert am 18.03.2020, zuletzt geprüft am 10.02.2022.

Sparks, C. (2003): Are the Western Media Really That Interested in China? In: Javnost – The Public 10 (4), S. 93–108.

Sperling, Valerie (2016): Putin's macho personality cult. In: Communist and Post-Communist Studies 49 (1), S. 13–23.

Spiegel, Steven L. (1983): Israel as a strategic asset. In: Commentary 75 (6), S. 51.

Spiegel Politik (2015): Russland erklärt US-Organisationen für unerwünscht. Hg. v. Spiegel Politik. Online verfügbar unter https://www.spiegel.de/politik/ausland/russland-erklaert-us-organisationen-fuer-unerwuenscht-a-1065291.html, zuletzt aktualisiert am 30.11.2015.

Spindler, Manuela (2014): Interdependence. In: Siegfried Schieder und Manuela Spindler (Hg.): Theories of international relations. London: Routledge, S. 56–75.

Staff, Toi (2020): Israel aghast at Iran cyberattack on civilian water infrastructure — TV report. Hg. v. Times of Israel. Online verfügbar unter https://www.timesofisrael.com/israel-aghast-at-iran-cyberattack-on-civilian-water-infrastructure-tv-report/, zuletzt aktualisiert am 09.05.2020, zuletzt geprüft am 07.10.2021.

Staniland, Paul (2015): Militias, Ideology, and the State. In: Journal of Conflict Resolution 59 (5), S. 770–793. DOI: 10.1177/0022002715576749.

Starks, Tim (2016): Obama administration accuses Russian government of election-year hacking. Hg. v. Politico. Online verfügbar unter https://www.politico.com/story/2016/10/obama-administration-accuses-russian-government-of-election-year-hacking-229296, zuletzt aktualisiert am 08.10.2016, zuletzt geprüft am 02.09.2021.

Stathis N. Kalyvas (1999): THE DECAY AND BREAKDOWN OF COMMUNIST ONE-PARTY SYSTEMS. In: Annual Review of Political Science 2 (1), S. 323–343. DOI: 10.1146/annurev.polisci.2.1.323.

Steffens, Timo (2018): Auf der Spur der Hacker. Wie man die Täter hinter der Computer-Spionage enttarnt. Berlin: Springer Vieweg.

Steffens, Timo (2020): Attribution of advanced persistent threats. How to identify the actors behind cyber-espionage. Berlin, Heidelberg: Springer Vieweg.

Steiger, Stefan; Harnisch, Sebastian; Zettl, Kerstin; Lohmann, Johannes (2018): Conceptualising conflicts in cyberspace. In: Journal of Cyber Policy 3 (1), S. 77–95. DOI: 10.1080/23738871.2018.1453526.

Stein, Jeff (2017): Exclusive: Russian Hackers Attacked the 2008 Obama Campaign. Hg. v. Newsweek. Online verfügbar unter https://www.newsweek.com/russia-hacking-trump-clinton-607956, zuletzt aktualisiert am 12.05.2017.

Stern (2019): Unit 8200 – diese Cyber-Soldaten sind der Motor für Israels Techboom. Hg. v. Stern. Online verfügbar unter https://www.stern.de/digital/online/unit-8200---diese-cyber-soldaten-sind-der-motor-fuer-israels-techboom-8757932.html, zuletzt aktualisiert am 18.06.2019, zuletzt geprüft am 25.10.2021.

Sternstein, Aliya (2016): DHS: Cyberattack on the Ukraine Power Grid Could Happen Here. Hg. v. Nextgov. Online verfügbar unter https://www.nextgov.com/cybersecurity/2016/04/dhs-ukraine-cyberattack-power-grid-could-happen-here/127262/, zuletzt aktualisiert am 06.04.2016, zuletzt geprüft am 29.09.2021.

Stewart, Will (2009): Were Russian security services behind the leak of ›Climategate‹ emails? Hg. v. Dailymail. Online verfügbar unter https://www.dailymail.co.uk/news/article-1233562/Emails-rocked-climate-change-campaign-leaked-Siberian-closed

-city-university-built-KGB.html, zuletzt aktualisiert am 06.12.2009, zuletzt geprüft am 19.05.2021.

Stoler, Yoav (2018): Israel to Train High Schoolers for Big Data Intelligence Jobs. Hg. v. Ctech. Online verfügbar unter https://www.calcalistech.com/ctech/articles/0,7340,L-3728778,00.html, zuletzt aktualisiert am 03.01.2018, zuletzt geprüft am 25.10.2021.

Stone, Jeff (2015a): Chinese Government Suspected In GitHub Hack, Evidence Links DDoS Attack To Censorship Push. Hg. v. International Business Times. Online verfügbar unter https://www.ibtimes.com/chinese-government-suspected-github-hack-evidence-links-ddos-attack-censorship-push-1863556, zuletzt aktualisiert am 30.03.2015, zuletzt geprüft am 02.08.2021.

Stone, Jeff (2015b): Meet CyberBerkut, The Pro-Russian Hackers Waging Anonymous-Style Cyberwarfare Against Ukraine. Online verfügbar unter https://www.ibtimes.com/meet-cyberberkut-pro-russian-hackers-waging-anonymous-style-cyberwarfare-against-2228902, zuletzt aktualisiert am 17.12.2015, zuletzt geprüft am 19.04.2021.

Stracqualursi, Veronica (2017): 10 times Trump attacked China and its trade relations with the US. Hg. v. ABC News. Online verfügbar unter https://abcnews.go.com/Politics/10-times-trump-attacked-china-trade-relations-us/story?id=46572567, zuletzt aktualisiert am 09.11.2017, zuletzt geprüft am 01.10.2021.

Strauss, Daniel (2016): Russian government hackers broke into DNC servers, stole Trump oppo. Hg. v. Politico. Online verfügbar unter https://www.politico.com/story/2016/06/russian-government-hackers-broke-into-dnc-servers-stole-trump-oppo-224315, zuletzt aktualisiert am 14.06.2016, zuletzt geprüft am 20.08.2021.

Stubbs, Jack; Bing, Christopher (2019): Hacking the hackers: Russian group hijacked Iranian spying operation, officials say. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK, zuletzt aktualisiert am 21.10.2019, zuletzt geprüft am 14.04.2021.

Stykow, Petra (2006): Gesellschaft als staatliche Veranstaltung? Unternehmerverbände und Staat in Rußland. In: Osteuropa 56 (9), S. 25–42. Online verfügbar unter https://www.jstor.org/stable/44934083.

Sukhankin, Sergey (2018): ›Continuing War by Other Means‹: The Case of Wagner, Russia's Premier Private Military Company in the Middle East. Jamestown Foundation. Online verfügbar unter https://jamestown.org/program/continuing-war-by-other-means-the-case-of-wagner-russias-premier-private-military-company-in-the-middle-east/, zuletzt geprüft am 11.06.2020.

Swed, Ori; Butler, John Sibley (2015): Military Capital in the Israeli Hi-tech Industry. In: Armed Forces & Society 41 (1), S. 123–141. DOI: 10.1177/0095327X13499562.

Symantec (2018): Thrip: Espionage Group Hits Satellite, Telecoms, an Defense Companies. Hg. v. Symantec. Online verfügbar unter https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets, zuletzt aktualisiert am 19.06.2018.

Tagesschau (2009): Russland: Medwedjew kippt schärferes Mediengesetz. Hg. v. Tagesschau. Online verfügbar unter http://www.tagesschau.de/ausland/medwedew26.html, zuletzt aktualisiert am 12.12.2009, zuletzt geprüft am 19.05.2021.

Tanase, Stefan (2015): Turla in the Sky: Satelliten-C&C. Hg. v. Kaspersky. Online verfügbar unter https://de.securelist.com/satellite-turla-apt-command-and-control-in-the-sky/65255/, zuletzt aktualisiert am 09.09.2015, zuletzt geprüft am 14.04.2021.

Tang, Rose (2001): China-U.S. cyber war escalates. Hg. v. CNN. Online verfügbar unter https://edition.cnn.com/2001/WORLD/asiapcf/east/04/27/china.hackers/index.html, zuletzt aktualisiert am 01.05.2001, zuletzt geprüft am 02.07.2021.

Tanriverdi, Hakan (2018): »Der Mythos vom anonymen Hacken wankt«. Hg. v. Süddeutsche Zeitung. Online verfügbar unter https://www.sueddeutsche.de/digital/cyberangriffe-der-mythos-vom-anonymen-hacken-wankt-1.3868826, zuletzt aktualisiert am 16.02.2018, zuletzt geprüft am 20.04.2021.

Tanriverdi, Hakan; Eckert, Svea; Strozyk, Jan; Zierer, Maximilian; Ciesielski, Rebecca (2019): Winnti: Attacking the Heart of the German Industry. Hg. v. Bayerischer Rundfunk. Online verfügbar unter https://web.br.de/interaktiv/winnti/english/, zuletzt aktualisiert am 24.07.2019, zuletzt geprüft am 25.06.2021.

TeamPassword (2021): Who is Deep Panda and how can you protect yourself? Hg. v. TeamPassword. Online verfügbar unter https://www.teampassword.com/blog/who-is-deep-panda-and-how-can-you-protect-yourself, zuletzt aktualisiert am 31.08.2021, zuletzt geprüft am 12.11.2021.

Temple-Raston, Dina (2019): How the U.S. hacked ISIS. Hg. v. National Public Radio. Online verfügbar unter https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis?t=1576775524015.

Tendler, Idan (2015): From The Israeli Army Unit 8200 To Silicon Valley. Hg. v. Techcrunch. Online verfügbar unter https://techcrunch.com/2015/03/20/from-the-8200-to-silicon-valley/, zuletzt aktualisiert am 20.03.2015, zuletzt geprüft am 11.10.2021.

Tertytchnaya, Katerina (2020): Protests and Voter Defections in Electoral Autocracies: Evidence From Russia. In: Comparative Political Studies 53 (12), S. 1926–1956. DOI: 10.1177/0010414019843556.

The Bell (2017): Прототип космического корабля для полетов на Марс от SpaceX Илона Маска впервые совершил успешную посадку — The Bell [Wie Amerika von den »russischen Hackern« erfuhr]. Hg. v. The Bell. Online verfügbar unter https://thebell.io/prototip-kosmicheskogo-korablya-dlya-poletov-na-mars-ot-spacex-ilona-maska-vpervye-sovershil-uspeshnuyu-posadku, zuletzt aktualisiert am 05.12.2017, zuletzt geprüft am 06.05.2021.

The Guardian (2007): Barack Obama's campaign speech. Hg. v. The Guardian. Online verfügbar unter https://www.theguardian.com/world/2007/feb/10/barackobama, zuletzt aktualisiert am 10.02.2007, zuletzt geprüft am 27.09.2021.

The Hague Program on International Cyber Security (2022): Closing the Gap 2022 | Responsibility in Cyberspace: Narratives and Practice. Call for Papers. Hg. v. Leiden University. Online verfügbar unter https://www.thehagueprogram.nl/news/closing-the-gap-2022-responsibility-in-cyberspace-narratives-and-practice, zuletzt geprüft am 12.02.2022.

The Jerusalem Post (2012): Israel among top arms exporters and importers. Hg. v. The Jerusalem Post. Online verfügbar unter https://www.jpost.com/Defense/Israel-among-top-arms-exporters-and-importers, zuletzt aktualisiert am 28.08.2012, zuletzt geprüft am 02.01.2022.

The New York Times (2009): WikiLeaks Archive — A Selection From the Cache of Diplomatic Dispatches. China's Ties to the World of Computer Hackers. Hg. v. The New York Times. Online verfügbar unter https://archive.nytimes.com/www.nytimes.com/interactive/2010/11/28/world/20101128-cables-viewer.html#report/china-09STATE67105, zuletzt aktualisiert am 19.06.2011, zuletzt geprüft am 02.07.2021.

The Straits Times (2017): Having Chinese Communist Party membership is like having ›a diploma‹, ›opens doors‹. Hg. v. The Straits Times. Online verfügbar unter https://www.straitstimes.com/asia/east-asia/having-chinese-communist-party-membership-is-like-having-a-diploma-and-opens-doors, zuletzt aktualisiert am 21.10.2017, zuletzt geprüft am 09.07.2021.

The Wall Street Journal (2016): China's ›White-Hat‹ Hackers Fear Dark Times After Community Founder Is Detained. Hg. v. The Wall Street Journal. Online verfügbar unter https://www.wsj.com/articles/BL-CJB-29440, zuletzt aktualisiert am 01.08.2016, zuletzt geprüft am 11.10.2021.

The White House (2009a): Remarks by the President on Securing Our Nation's Cyber Infrastructure. Hg. v. The White House. Online verfügbar unter https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure, zuletzt aktualisiert am 02.03.2010, zuletzt geprüft am 24.08.2021.

The White House (2009b): The Comprehensive National Cybersecurity Initiative. Hg. v. The White House. Online verfügbar unter https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative, zuletzt geprüft am 24.08.2021.

The White House (2021): The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China. Online verfügbar unter https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/, zuletzt aktualisiert am 19.07.2021, zuletzt geprüft am 01.10.2021.

Thomas, Neil (2020): Members Only: A Look at Recruitment Trends in the CCP. Hg. v. MacroPolo. Online verfügbar unter https://macropolo.org/analysis/members-only-recruitment-trends-in-the-chinese-communist-party/, zuletzt aktualisiert am 15.07.2020, zuletzt geprüft am 09.07.2021.

Thomas Colatin, Samuele de (2019): Power grid cyberattack in Ukraine (2015) – International cyber law: interactive toolkit. Hg. v. CCDCOE. Online verfügbar unter https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015), zuletzt aktualisiert am 17.05.2019, zuletzt geprüft am 16.04.2021.

Threat Connect Research Team (2016): Does a BEAR Leak in the Woods? Hg. v. ThreatConnect. Online verfügbar unter https://threatconnect.com/blog/does-a-bear-leak-in-the-woods/#post_content, zuletzt aktualisiert am 12.08.2016, zuletzt geprüft am 20.08.2021.

ThreatConnect (2015): Project Camerashy. Closing the Aperture on China's Unit 78020. Hg. v. ThreatConnect. Online verfügbar unter https://cdn2.hubspot.net/hubfs/454298/Project_CAMERASHY_ThreatConnect_Copyright_2015.pdf, zuletzt geprüft am 02.07.2021.

ThreatConnect (2016): Belling the BEAR. Hg. v. ThreatConnect Insights. ThreatConnect. Online verfügbar unter https://threatconnect.com/blog/russia-hacks-belling cat-mh17-investigation/, zuletzt aktualisiert am 28.09.2016, zuletzt geprüft am 20.04.2021.

ThreatExpert (2008): ThreatExpert Blog: Agent.btz – A Threat That Hit Pentagon. Hg. v. ThreatExpert. Online verfügbar unter http://blog.threatexpert.com/2008/11/agen tbtz-threat-that-hit-pentagon.html, zuletzt aktualisiert am 28.02.2020, zuletzt geprüft am 14.04.2021.

TMG (2014): About Us. Hg. v. Tianji Media Group. Online verfügbar unter http://www.ti anjimedia.com/english/.

Tobin, Liza (2018): Xi's Vision for Transforming Global Governance: A Strategic Challenge for Washington and Its Allies (November 2018). In: Texas National Security Review 2 (1). DOI: 10.26153/TSW/863.

Top Universities (2020): Computer Science and Information Systems 2020. Hg. v. Top Universities. Online verfügbar unter https://www.topuniversities.com/university-r ankings/university-subject-rankings/2020/computer-science-information-system s, zuletzt aktualisiert am 24.08.2021, zuletzt geprüft am 24.08.2021.

Torbati, Yeganeh (2016): Trump election puts Iran nuclear deal on shaky ground. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-usa-election-t rump-iran-idUSKBN13427E, zuletzt aktualisiert am 09.11.2016, zuletzt geprüft am 06.10.2021.

Treisman, Daniel (2007): Putin's silovarchs. In: Orbis 51 (1), S. 141–153.

Tress, Luke (2021): Chinese group carried out widespread cyber espionage campaign in Israel. Hg. v. The Times of Israel. Online verfügbar unter https://www.timesofisrael .com/chinese-group-carried-out-widespread-cyber-espionage-campaign-in-israel -report/, zuletzt aktualisiert am 10.08.2021, zuletzt geprüft am 12.02.2022.

Troianovski, Anton (2021): China Censors the Internet. So Why Doesn't Russia? Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2021/02/21 /world/europe/russia-internet-censorship.html, zuletzt aktualisiert am 10.03.2021, zuletzt geprüft am 05.05.2021.

Troianovski, Anton; Nakashima, Ellen (2018): How Russia's military intelligence agency became the covert muscle in Putin's duels with the West. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpost.com/world/europe/ho w-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-du els-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html, zuletzt aktualisiert am 28.12.2018, zuletzt geprüft am 12.05.2021.

Tse, Don (2018): Why General Fang Fenghui Was Purged. Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2018/01/why-general-fang-fenghui-was-pur ged/, zuletzt aktualisiert am 14.01.2018, zuletzt geprüft am 31.07.2021.

Tsygankov, Andrei P. (2019): Russia and America. The asymmetric rivalry. Cambridge, UK, Medford, MA, USA: Polity.

Tucker, Patrick (2018): Russia Launched Cyber Attacks Against Ukraine Before Ship Seizures, Firm Says. Hg. v. DefenseOne. Online verfügbar unter https://www.defen seone.com/technology/2018/12/russia-launched-cyber-attacks-against-ukraine-shi

p-seizures-firm-says/153375/, zuletzt aktualisiert am 07.12.2018, zuletzt geprüft am 28.04.2021.

U.S. Government (2007): Blackwater USA. Hearing before the Committee on Oversight and Government Reform. Hg. v. U.S. Government Printing Office. House of Representatives. Washington, D.C. Online verfügbar unter https://oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/20071127131151.pdf, zuletzt aktualisiert am 02.10.2007, zuletzt geprüft am 23.04.2020.

U.S. Mission Korea (2017): Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea. Hg. v. U.S. Embassy & Consulate in the Republic of Korea. Online verfügbar unter https://kr.usembassy.gov/121917-press-briefing-attribution-wannacry-malware-attack-north-korea/, zuletzt aktualisiert am 19.12.2017, zuletzt geprüft am 07.01.2022.

Umland, Andreas (2021): Würde ein Präsident Alexei Nawalny die Krim zurückgeben? Hg. v. Neue Züricher Zeitung. Online verfügbar unter https://www.nzz.ch/meinung/wuerde-ein-praesident-alexei-nawalny-die-krim-zurueckgeben-ld.1600611, zuletzt aktualisiert am 10.02.2021, zuletzt geprüft am 06.05.2021.

Ungerleider, Neal (2013): How Check Point Became The Fortune 500's Cybersecurity Favorite. Hg. v. Fast Company. Online verfügbar unter https://www.fastcompany.com/3012414/how-check-point-became-the-fortune-500s-cybersecurity-favorite, zuletzt aktualisiert am 04.06.2013, zuletzt geprüft am 11.10.2021.

UNODC (2019): Cyberespionage. Hg. v. United Nations Office on Drugs and Crime (E4J University Module Series: Cybercrime. Module 14: Hacktivism, Terrorism, Espionage, Disinformation Campaigns and Warfare in Cyberspace). Online verfügbar unter https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberespionage.html, zuletzt aktualisiert am Juni 2019.

US Cyber Command (o.J.): Command History. Hg. v. US Cyber Command. Online verfügbar unter https://www.cybercom.mil/About/History/, zuletzt aktualisiert am 25.08.2021, zuletzt geprüft am 25.08.2021.

US Government (2014): H. R. 5103. Hg. v. U.S. Government Publishing Office. US Congress. Online verfügbar unter https://www.govinfo.gov/content/pkg/BILLS-113hr5103ih/html/BILLS-113hr5103ih.htm, zuletzt aktualisiert am 14.07.2014, zuletzt geprüft am 12.08.2021.

US Joint Chiefs of Staff (1998): Joint Pub 3–13: Joint Doctrine for Information Operations, October 9, 1998. Hg. v. US Joint Chiefs of Staff US Joint Chiefs of Staff. Online verfügbar unter https://www.hsdl.org/?abstract&did=3759, zuletzt geprüft am 24.08.2021.

US Senate (o.J.): About Treaties. Hg. v. United States Senate. Online verfügbar unter https://www.senate.gov/about/powers-procedures/treaties.htm, zuletzt geprüft am 25.08.2021.

Valache, Carmen (2020): Israel's Unit 8200 trains highly skilled entrepreneurs, who move on to set up cyber defense and autonomous veh. Hg. v. Interesting Engineering. Online verfügbar unter https://interestingengineering.com/israels-unit-8200-a-conveyor-belt-of-high-tech-startups, zuletzt aktualisiert am 17.08.2020, zuletzt geprüft am 25.10.2021.

Valeriano, Brandon (2021): Does the Cyber Offense Have the Advantage? Hg. v. Offensive Cyber Working Group. Online verfügbar unter https://offensivecyber.org/2021/12/2

o/does-the-cyber-offense-have-the-advantage/, zuletzt aktualisiert am 20.12.2021, zuletzt geprüft am 17.01.2022.

Valeriano, Brandon; Jensen, Benjamin (2019): The Myth of the Cyber Offense: The Case for Cyber Restraint. In: Cato Institute Policy Analysis (862).

Valeriano, Brandon; Jensen, Benjamin M.; Maness, Ryan C. (2018): Cyber strategy. The evolving character of power and coercion. New York, NY: Oxford University Press. Online verfügbar unter http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=1776310.

Valeriano, Brandon; Maness, Ryan (2015): Cyber war versus cyber realities. Cyber conflict in the international system. Oxford, New York: Oxford University Press.

Valeriano, Brandon; Maness, Ryan C. (2014): The dynamics of cyber conflict between rival antagonists, 2001–11. In: Journal of Peace Research 51 (3), S. 347–360. DOI: 10.1177/0022343313518940.

Valeriano, Brandon; Maness, Ryan C. (2018): How We Stopped Worrying about Cyber Doom and Started Collecting Data. In: PaG 6 (2), S. 49. DOI: 10.17645/pag.v6i2.1368.

Välisluureamet (2018): International Security and Estonia 2018. Hg. v. Estonian Foreign Intelligence Service. Online verfügbar unter https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf, zuletzt geprüft am 14.04.2021.

Value (2021): World Top Technology Companies by Market Value as on 2020. Hg. v. Value. Online verfügbar unter https://www.value.today/world-top-companies/technology?title=&field_headquarters_of_company_target_id&field_company_category_primary_target_id&field_market_value_jan_2020_value_1=&page=0, zuletzt geprüft am 25.08.2021.

van Apeldoorn, Bastiaan; Graaff, Naná de (2014): Corporate elite networks and US post-Cold War grand strategy from Clinton to Obama. In: European Journal of International Relations 20 (1), S. 29–55. DOI: 10.1177/1354066111433895.

van Apeldoorn, Bastiaan; Graaff, Naná de (2017): Obama's economic recovery strategy open markets and elite power: business as usual? In: Int Polit 54 (3), S. 356–372. DOI: 10.1057/s41311-017-0030-3.

van Rosenthal, Eelco Bosch (2018): Dutch intelligence first to alert U.S. about Russian hack of Democratic Party. Hg. v. NOS. Online verfügbar unter https://nos.nl/nieuwsuur/artikel/2213767-dutch-intelligence-first-to-alert-u-s-about-russian-hack-of-democratic-party.html, zuletzt aktualisiert am 25.01.2018, zuletzt geprüft am 14.04.2021.

vander Straeten, Pascal (2020): Treatise On China's Clandestine Financial Warfare: China's Intelligence Community And The Communist Party As Key Players In Geofinance In The 21st Century«. Dallas Fort Worth, Texas: Value4Risk LLC.

Vavra, Shannon (2019): How did a Chinese APT get a U.S. hacking tool before it was leaked? Check Point has a theory. Hg. v. Cyberscoop. Online verfügbar unter https://www.cyberscoop.com/apt3-nsa-tools-smb-check-point/, zuletzt aktualisiert am 05.09.2019, zuletzt geprüft am 30.06.2021.

Voo, Julia; Hemani, Irfan; Jones, Simon; DeSombre, Winnona; Cassidy, Daniel; Schwarzenbach, Anna (2020): National Cyber Power Index 2020. Methodology and Analytical Considerations. Hg. v. Harvard Kennedy School, Belfer Center for Science and International Affairs. Online verfügbar unter https://www.belfercenter.org/p

ublication/national-cyber-power-index-2020#:~:text=The%20Belfer%20National %20Cyber%20Power,collected%20from%20publicly%20available%20data., zuletzt aktualisiert am 2020, zuletzt geprüft am 25.01.2021.

Walker, Shaun (2017): Ex-minister's harsh jail sentence sends shockwaves through Russian elite. Hg. v. The Guardian. Online verfügbar unter https://www.theguardia n.com/world/2017/dec/15/russia-jails-former-economy-minister-alexei-ulyukayev-for-corruption, zuletzt aktualisiert am 15.12.2017, zuletzt geprüft am 12.05.2021.

Walton, Calder (2018): Russia has a long history of eliminating ›enemies of the state‹. Hg. v. The Washington Post. Online verfügbar unter https://www.washingtonpo st.com/news/monkey-cage/wp/2018/03/13/russia-has-a-long-history-of-eliminat ing-enemies-of-the-state/, zuletzt aktualisiert am 13.03.2018, zuletzt geprüft am 14.04.2021.

Wang, Zheng (2014): The Chinese dream: Concept and context. In: Journal of Chinese Political Science 19 (1), S. 1–13.

Warrick, Joby; Nakashima, Ellen (2020): Officials: Israel linked to a disruptive cyberattack on Iranian port facility. Hg. v. The Washington Post. Online verfügbar unter h ttps://www.washingtonpost.com/national-security/officials-israel-linked-to-a-di sruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89f d-28fb313d1886_story.html, zuletzt aktualisiert am 18.05.2020, zuletzt geprüft am 07.10.2021.

Wassermann, Felix (2014): Asymmetrische Kriege. Dissertation. Humboldt-Universität, Berlin.

Watanabe, Daisuke; Schmitz, Peter (2021): 4 Tipps zur Bekämpfung von »Living-off-the-Land«-Angriffe. Hg. v. Security-Insider. Online verfügbar unter https://www.securi ty-insider.de/4-tipps-zur-bekaempfung-von-living-off-the-land-angriffe-a-10460 09/, zuletzt aktualisiert am 10.08.2021, zuletzt geprüft am 17.01.2022.

Watkins, Ali (2017): Obama team was warned in 2014 about Russian interference. Hg. v. Politico. Online verfügbar unter https://www.politico.com/story/2017/08/14/obama -russia-election-interference-241547, zuletzt aktualisiert am 14.08.2017, zuletzt geprüft am 08.09.2021.

Waxman, Dov (2009): From Jerusalem to Baghdad? Israel and the War in Iraq. In: International Studies Perspectives 10 (1), S. 1–17. Online verfügbar unter http://www.jsto r.org/stable/44218575.

Wehle, Kimberly (2020): The Checks and Balances That Trump Has Swept Away. Hg. v. The Atlantic. Online verfügbar unter https://www.theatlantic.com/ideas/archive/ 2020/02/checks-and-balances-trump-has-swept-away/606013/, zuletzt aktualisiert am 04.02.2020, zuletzt geprüft am 26.08.2021.

Weiss, Michael (2020): AQUARIUM LEAKS Inside the GRU's Psychological Warfare Program. Hg. v. Free Russia Foundation. Washington, DC. Online verfügbar unter https://www.4freerussia.org/aquarium-leaks-inside-the-gru-s-psychological -warfare-program/.

WeLiveSecurity (2019): Operation Ghost: The Dukes aren't back – they never left | WeLiveSecurity. Hg. v. ESET. Online verfügbar unter https://www.welivesecurity.com /2019/10/17/operation-ghost-dukes-never-left/, zuletzt aktualisiert am 01.10.2020, zuletzt geprüft am 13.04.2021.

Wen, Philip (2017): China denies links to alleged cyber attacks in United States targeting exiled tycoon Guo. Hg. v. Reuters. Online verfügbar unter https://www.reuters.com/article/us-china-corruption-tycoon-idUSKBN1CD0AP, zuletzt aktualisiert am 08.10.2017, zuletzt geprüft am 04.08.2021.

Whyte, Christopher (2018): Dissecting the Digital World: A Review of the Construction and Constitution of Cyber Conflict Research. In: International Studies Review 20 (3), S. 520–532. DOI: 10.1093/isr/viw013.

Wiegand, Dorothee (2014): Milliardendeal: Sicherheitsfirma FireEye übernimmt Mandiant. Hg. v. Heise Online. Online verfügbar unter https://www.heise.de/security/meldung/Milliardendeal-Sicherheitsfirma-FireEye-uebernimmt-Mandiant-2075120.html, zuletzt aktualisiert am 04.01.2014, zuletzt geprüft am 12.08.2021.

Wilkie, Christina (2021): Biden presses Putin to disrupt cybercriminals in Russia as U.S. grapples with latest ransomware attacks. Hg. v. CNBC. Online verfügbar unter https://www.cnbc.com/2021/07/09/ransomware-biden-presses-putin-to-disrupt-cybercriminals-in-russia.html, zuletzt aktualisiert am 09.07.2021, zuletzt geprüft am 05.08.2021.

William J. Lynn III (2010): Defending a New Domain. The Pentagon's Cyberstrategy. Hg. v. Foreign Affairs. Online verfügbar unter https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain, zuletzt aktualisiert am 01.09.2010, zuletzt geprüft am 14.04.2021.

Williams, Nick (2020): Rockwell to expand cyber services through acquisition of Israeli company. Hg. v. Milwaukee Business Journal. Online verfügbar unter https://www.bizjournals.com/milwaukee/news/2020/01/08/rockwell-to-expand-cyber-services-through.html, zuletzt aktualisiert am 08.01.2020, zuletzt geprüft am 03.11.2021.

WinTotal (2020): Einfach erklärt: Was ist ein Root-Server? Hg. v. WinTotal.de. Online verfügbar unter https://www.wintotal.de/root-server/, zuletzt aktualisiert am 06.08.2021, zuletzt geprüft am 16.01.2022.

Wipperfürth, Christian (2011): Außenpolitik unter Präsident Dmitri Medwedew (2008–2011). In: Christian Wipperfürth (Hg.): Russlands Außenpolitik. 1. Aufl. Wiesbaden: VS Verl. für Sozialwiss (Lehrbuch), S. 101–119.

Wong, Edward; Buckley, Chris (2021): U.S. Says China's Repression of Uighurs Is ›Genocide‹. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2021/01/19/us/politics/trump-china-xinjiang.html, zuletzt aktualisiert am 19.01.2021, zuletzt geprüft am 30.07.2021.

Woo, Stu; Wexler, Alexandra (2021): U.S.-China Tech Fight Opens New Front in Ethiopia. Hg. v. The Straits Times. Online verfügbar unter https://www.wsj.com/articles/u-s-china-tech-fight-opens-new-front-in-ethiopia-11621695273, zuletzt aktualisiert am 22.05.2021, zuletzt geprüft am 04.08.2021.

Work, J. D. (2021): China Flaunts Its Offensive Cyber Power – War on the Rocks. Hg. v. War on the Rocks. Online verfügbar unter https://warontherocks.com/2021/10/china-flaunts-its-offensive-cyber-power/, zuletzt aktualisiert am 22.10.2021, zuletzt geprüft am 25.10.2021.

Work, J. D.; Harknett, Richard (2020): Troubled vision: Understanding recent Israeli–Iranian offensive cyber exchanges. Hg. v. Atlantic Council. Online verfügbar unter https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/trouble

d-vision-understanding-israeli-iranian-offensive-cyber-exchanges/, zuletzt aktualisiert am 22.07.2020, zuletzt geprüft am 03.01.2022.

World Bank (2020): High-technology exports (% of manufactured exports) – China. Hg. v. World Bank. Online verfügbar unter https://data.worldbank.org/indicator/TX.VAL.TECH.MF.ZS?locations=CN, zuletzt geprüft am 26.04.2021.

World Bank (2021a): High-technology exports (% of manufactured exports). Hg. v. World Bank. Online verfügbar unter https://data.worldbank.org/indicator/TX.VAL.TECH.MF.ZS, zuletzt geprüft am 28.04.2021.

World Bank (2021b): High-technology exports (% of manufactured exports) – United States, China. Hg. v. World Bank. Online verfügbar unter https://data.worldbank.org/indicator/TX.VAL.TECH.MF.ZS?locations=US-CN, zuletzt geprüft am 25.08.2021.

World Bank (2021c): Research and Development Expenditure. Hg. v. World Bank. Online verfügbar unter https://databank.worldbank.org/reports.aspx?source=2&series=GB.XPD.RSDV.GD.ZS#, zuletzt aktualisiert am 26.04.2021, zuletzt geprüft am 26.04.2021.

World Bank (2021d): Research and development expenditure (% of GDP) – United States, China. Hg. v. World Bank. Online verfügbar unter https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=US-CN, zuletzt geprüft am 25.08.2021.

World Bank (2022a): High-technology exports (% of manufactured exports) – Israel. Hg. v. World Bank. Online verfügbar unter https://data.worldbank.org/indicator/TX.VAL.TECH.MF.ZS?locations=IL, zuletzt aktualisiert am 02.01.2022, zuletzt geprüft am 02.01.2022.

World Bank (2022b): Research and development expenditure (% of GDP) – Israel. Hg. v. World Bank. Online verfügbar unter https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=IL, zuletzt aktualisiert am 02.01.2022, zuletzt geprüft am 02.01.2022.

Wortham, Jenna (2016): Obama Brought Silicon Valley to Washington. Hg. v. The New York Times. Online verfügbar unter https://www.nytimes.com/2016/10/30/magazine/barack-obama-brought-silicon-valley-to-washington-is-that-a-good-thing.html?, zuletzt aktualisiert am 25.10.2016, zuletzt geprüft am 02.09.2021.

Wright, Thomas (2017): All measures short of war: the contest for the twenty-first century and the future of American power: Yale University Press.

Wuthnow, Joel; Saunders, Phillip Charles (2017): Chinese military reform in the age of Xi Jinping: Drivers, challenges, and Implications. Hg. v. Institute for National Strategic Studies. Center for the Study of Chinese Military Affairs. Washington, D.C. (China Strategic Perspectives, 10). Online verfügbar unter https://apps.dtic.mil/sti/pdfs/AD1030342.pdf, zuletzt geprüft am 02.08.2021.

Xinhua (2013): Xi Jinping leitete das Treffen, um die Entwicklung und das Management der Parteimitglieder unter der neuen Situation zu stärken. Hg. v. The Central People's Government of the People´s Republic of China. Online verfügbar unter http://www.gov.cn/ldhd/2013-01/28/content_2321165.htm, zuletzt aktualisiert am 28.01.2013, zuletzt geprüft am 09.07.2021.

Yakovlev, Andrey (2020): The Dark Side of Russia: How New Internet Laws and Nationalism Fuel Russian Cybercrime. Hg. v. IntSights. Online verfügbar unter https://int

sights.com/resources/how-new-internet-laws-and-nationalism-fuel-russian-cybercrime, zuletzt aktualisiert am 20.05.2021, zuletzt geprüft am 20.05.2021.

Yeisley, Mark O. (2011): Bipolarity, proxy wars, and the rise of China. In: Strategic Studies Quarterly 5 (4), S. 75–91.

Yerman, Jordan (2019): A Startup Nation: Why Israel Has Become The New Silicon Valley. Hg. v. APEX. Online verfügbar unter https://apex.aero/articles/startup-nation-israel-become-silicon-valley/, zuletzt aktualisiert am 22.05.2019, zuletzt geprüft am 26.10.2021.

Yozma (2021): Overview. Hg. v. Yozma. Online verfügbar unter https://www.yozma.com/overview/, zuletzt geprüft am 26.10.2021.

Zacher, Mark W.; Matthew, Richard A. (1995): Liberal international theory: common threads, divergent strands. In: Charles W. Kegley (Hg.): Controversies in international relations theory. Realism and the neoliberal challenge. New York, NY: St. Martin's Press, S. 107–149.

Zarroli, Jim (2018): It Was A Company With A Lot Of Promise. Then A Chinese Customer Stole Its Technology. Hg. v. NPR. Online verfügbar unter https://www.npr.org/2018/04/09/599557634/it-was-a-company-with-a-lot-of-promise-then-a-chinese-customer-stole-its-technol, zuletzt aktualisiert am 09.04.2018, zuletzt geprüft am 27.07.2021.

Zegart, Amy B. (2000): Flawed by design. The evolution of the CIA, JCS, and NSC. [Nachdr.]. Stanford, California: Stanford University Press.

Zerachovitz, Omri (2021): Israeli hi-tech startups are booming. This is what it takes to raise a unicorn. Hg. v. Haaretz. Online verfügbar unter https://www.haaretz.com/israel-news/business/.premium.MAGAZINE-israeli-hi-tech-startups-are-booming-this-is-what-it-takes-to-raise-a-unicorn-1.9662215, zuletzt aktualisiert am 30.03.2021, zuletzt geprüft am 26.10.2021.

Zetter, Kim (2014): Russian ›Sandworm‹ Hack Has Been Spying on Foreign Governments for Years. Hg. v. Wired. Online verfügbar unter https://www.wired.com/2014/10/russian-sandworm-hack-isight/?redirectURL=https%3A%2F%2Fwww.wired.com%2F2014%2F10%2Frussian-sandworm-hack-isight%2F, zuletzt aktualisiert am 14.10.2014, zuletzt geprüft am 19.05.2021.

Zetter, Kim (2017a): The Ukrainian Power Grid Was Hacked Again. Hg. v. Vice. Online verfügbar unter https://www.vice.com/en/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report, zuletzt aktualisiert am 10.01.2017, zuletzt geprüft am 16.04.2021.

Zetter, Kim (2017b): WikiLeaks Files Show the CIA Repurposing Hacking Code to Save Time, Not to Frame Russia. Hg. v. The Intercept. Online verfügbar unter https://theintercept.com/2017/03/08/wikileaks-files-show-the-cia-repurposing-foreignhacking-code-to-save-time-not-to-frame-russia/.

Zetter, Kim (2019): How Close Did Russia Really Come to Hacking the 2016 Election? Hg. v. Politico. Online verfügbar unter https://www.politico.com/news/magazine/2019/12/26/did-russia-really-hack-2016-election-088171, zuletzt aktualisiert am 26.12.2019, zuletzt geprüft am 05.05.2021.

Zettl, Kerstin (2019): Lesson learned? Demokratische Resilienz gegenüber digitaler Wahlbeeinflussung in den USA und Deutschland. In: Zeitschrift für Außen- und Sicherheitspolitik 12 (4), S. 429–451. DOI: 10.1007/s12399-020-00789-7.

Zettl, Kerstin (2022): Der Einsatz von Cyberproxies zur Wahrung autokratischer Regimesicherheit – Iran und Nordkorea im Vergleich. In: Kerstin Zettl, Sebastian Harnisch und Mischa Hansel (Hg.): Asymmetrien in Cyberkonflikten. Wie Attribution und der Einsatz von Proxies die Normentwicklung beeinflussen. Baden-Baden: Nomos, S. 69 – 104.

Zezula, Ladislav; Kroustek, Jakub; Hron, Martin (2017): It's Rabbit season: BadRabbit ransomware infects airports and subways. Hg. v. Threat Intelligence Team. Avast. Online verfügbar unter https://blog.avast.com/its-rabbit-season-badrabbit-ransomware-infects-airports-and-subways, zuletzt aktualisiert am 25.10.2017, zuletzt geprüft am 19.04.2021.

Zheng, Yongnian; Tok, Sow Keat (2007): Harmonious society and harmonious world: China's policy discourse under Hu Jintao. In: Briefing Series 26, S. 1–12.

Zhou, Taomo (2015): Ambivalent Alliance: Chinese Policy towards Indonesia, 1960–1965. In: The China Quarterly 221, S. 208–228. DOI: 10.1017/s0305741014001544.

Zhu, Zhiqun (2020): Interpreting China's ›Wolf-Warrior Diplomacy‹. Hg. v. The Diplomat. Online verfügbar unter https://thediplomat.com/2020/05/interpreting-chinas-wolf-warrior-diplomacy/, zuletzt aktualisiert am 15.05.2020, zuletzt geprüft am 17.06.2021.

Abbildungsverzeichnis

Tabellenverzeichnis



Die Reihe wird herausgegeben von Jeanette Hofmann, Norbert Kersting, Claudia Ritzi und Wolf J. Schünemann.

Kerstin Zettl-Schabath, geb. 1993, ist Wissenschaftlerin am Institut für Politische Wissenschaft der Universität Heidelberg und arbeitet seit 2022 im Forschungsprojekt »European Repository of Cyber Incidents« (EuRepoC). Ihre Dissertation erhielt 2022 den Preis der Dr. Karl A. Lamers Friedens-Stiftung.

Politikwissenschaft



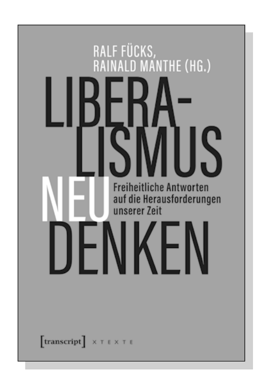
Knut Bergmann (Hg.)
»Mehr Fortschritt wagen«?
Parteien, Personen, Milieus und Modernisierung:
Regieren in Zeiten der Ampelkoalition

Juni 2022, 492 S., kart., 27 Farbabbildungen, 2 SW-Abbildungen
30,00 € (DE), 978-3-8376-6307-5
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-6307-9
ISBN 978-3-7328-6307-5



Pola Lehmann, Theres Matthieß,
Sven Regel, Bernhard Weßels
Die Ampelkoalition
Wie wird aus unterschiedlichen Zielen
ein gemeinsames Regierungsprogramm?

Juli 2022, 200 S., kart., 12 SW-Abbildungen, 2 Farbabbildungen
19,50 € (DE), 978-3-8376-6332-7
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-6332-1
ISBN 978-3-7328-6332-7



Ralf Fücks, Rainald Manthe (Hg.)
Liberalismus neu denken
Freiheitliche Antworten
auf die Herausforderungen unserer Zeit

Juni 2022, 202 S., kart.
19,50 € (DE), 978-3-8376-6319-8
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-6319-2
ISBN 978-3-7328-6319-8

Leseproben, weitere Informationen und Bestellmöglichkeiten
finden Sie unter www.transcript-verlag.de

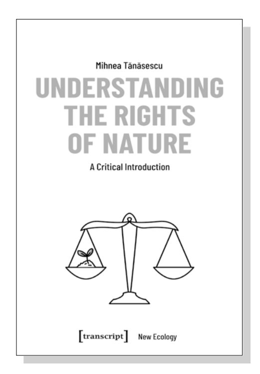
Politikwissenschaft



BICC Bonn International Centre for Conflict Studies, HSFK Leibniz-Institut Hessische Stiftung Friedens- und Konfliktforschung, IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, INEF Institut für Entwicklung und Frieden

Friedensgutachten 2022
Friedensfähig in Kriegszeiten

Juni 2022, 152 S., kart., 25 Farbabbildungen
15,00 € (DE), 978-3-8376-6403-4
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-6403-8



Mihnea Tanasescu

Understanding the Rights of Nature
A Critical Introduction

February 2022, 168 p., pb.
40,00 € (DE), 978-3-8376-5431-8
E-Book: available as free open access publication
PDF: ISBN 978-3-8394-5431-2



Gregor Ritschel

Freie Zeit
Eine politische Idee von der Antike bis zur Digitalisierung

2021, 274 S., kart.
28,00 € (DE), 978-3-8376-5572-8
E-Book: kostenlos erhältlich als Open-Access-Publikation
PDF: ISBN 978-3-8394-5572-2
ISBN 978-3-7328-5572-8

Leseproben, weitere Informationen und Bestellmöglichkeiten finden Sie unter www.transcript-verlag.de